Contents

Welcome to the Netopia S9500 Security Appliance *Reference Guide*. This guide is designed to be your single source for information about your Netopia S9500 Security Appliance. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

This Table of Contents page you are viewing consists of hypertext links to the chapters and headings listed. If you are viewing this on-line, just click any link below to go to that heading.

Chapter 1

Introduction

Overview

Welcome to the Netopia S9500 Security Appliance, the complete security solution for connecting your Ethernet local area network (LAN) to the Internet. The Netopia S9500 Security Appliance is a LAN-based product providing firewall, Virtual Private Network (VPN), and traffic shaping services at line rates up to 10 Mbps. The Netopia S9500 Security Appliance is a compact, desktop or rack-mountable platform, providing a complete security solution for valuable data.

This chapter covers the following topics:

- "Features and capabilities" on page 1-5
- "How to use this guide" on page 1-6

Features and capabilities

The Netopia S9500 Security Appliance provides the following features:

- Firewall: The Netopia S9500 Security Appliance is a full-featured firewall that combines the technologies from packet filters, proxy servers, and dynamic circuit-level packet filters. The firewall can screen TCP/IP packets and deny or grant access based on criteria such as IP address and TCP/IP protocol. You can manipulate these policies so that, for example, only data from certain addresses is allowed to pass through the firewall.
- VPN: A virtual private network, VPN, allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public internet to look "virtually" like a private secure network. Netopia S9500's VPN conforms to the Internet Protocol Security, IPSec, standard, ensuring that it is interoperable with other IPSec devices.
- IKE key management: The Netopia S9500 Security Appliance uses the IKE key management protocol. The IPSec and IKE protocol suites together provide everything you need for secure communications — authentication, integrity, and confidentiality — and make key exchange practical even in larger networks.
- Security: The Netopia S9500 Security Appliance with VPN supports DES and Triple-DES encryption and MD5 and SHA-1 authentication thus providing you with the highest level of security.
- Monitoring: The Netopia S9500 Security Appliance provides a comprehensive monitoring tool to identify network traffic inefficiencies and to monitor traffic flow in real-time. The prioritization management utility allows not only the ranking of processes based on the type of function being performed by the user, but also the limiting of users to a certain percentage of the global bandwidth available.
- Event reporting: The Netopia S9500 Security Appliance performs real-time event logging and alerting with unmatched reporting capabilities. All graphs of the usage data can be viewed with a Web browser on the Internet. The usage data can also be downloaded and imported to a spreadsheet or database for statistical analysis, usage-based accounting and billing.

- Easy integration: The Netopia S9500 Security Appliance can be placed anywhere in a 10BaseT LAN. Native support for IP ensures that the Netopia S9500 Security Appliance interoperates transparently with the broadest range of Intranet devices and other network applications.
- NAT: The use of network address translation (NAT) translates multiple IP addresses on the Trusted LAN to one public address that is sent out to the Internet (Untrusted interface). This adds a level of security since the addresses of hosts connected to the Trusted LAN are never provided to the Untrusted Network. Also, NAT preserves the use of IP addresses if not enough are provided by the ISP.
- Web management: The Netopia S9500 Security Appliance uses Web technology that provides a Web-server interface to the configuration and management system. Thus, you may use a fast and easy utility to access, monitor, and control your firewall configurations with standard Web browsers. You can also use the built-in Web server for remote configuration and management.
- SNMP and CLI management: The Netopia S9500 Security Appliance is also SNMP-compatible and therefore, can be managed by network administration software. Further, the Netopia S9500 Security Appliance allows script manipulation and modem control via a command line interface (CLI).

How to use this guide

In addition to the simple documentation contained in the accompanying documentation folio, this guide is designed to be your single source for information about your Netopia S9500 Security Appliance. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

You can also print out all of the manual, or individual sections, if you prefer to work from hard copy rather than on-line documentation. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on 3-hole punched paper, so that you can put the pages in a binder for future reference. For your convenience, a printed copy is available from Netopia. Order part number TER9500/Doc.

Chapter 2

Making the Physical Connections

This chapter tells you how to make the physical connections to your Netopia S9500 Security Appliance.

This chapter covers the following topics:

Find a location

When choosing a location for the S9500, consider:

- Available space and ease of installation
- Physical layout of the building and how to best use the physical space available in relation to connecting your S9500 to the LAN
- Available wiring and jacks
- Distance from the point of installation to the next device (length of cable or wall wiring)
- Ease of access to the front of the unit for configuration and monitoring
- Ease of access to the back of the unit for checking and changing cables
- Cable length and network size limitations when expanding networks
- Air circulation

For small networks, install the Netopia S9500 near one of the LANs. For large networks, you can install the Netopia S9500 in a wiring closet or a central network administration site.

What you need

Locate all items that you need for the installation. Included in your equipment package are:

- The Netopia S9500 Security Appliance
- A power adapter and cord with a mini-DIN8 connector
- Two Ethernet cables (RJ-45) to connect to a hub, router, or server
- A dual DB-25 and mini-DIN8 to DB-25 console cable (to connect the S9500 to either a PC or a Macintosh)
- The Netopia CD containing this documentation, an Internet browser, Adobe® Acrobat® Reader for Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet 2.6 for Macintosh

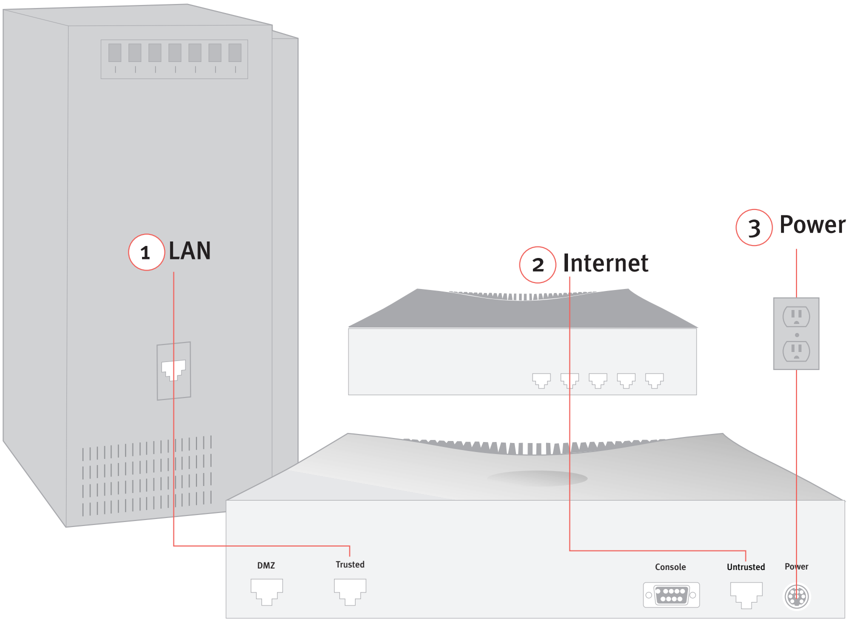
You will also need:

- A Windows 95, 98, or NT-based PC or a Macintosh with Ethernet connectivity for configuring the Netopia S9500. This may be built-in Ethernet or an add-on card, with TCP/IP installed.

Identify the connectors and attach the cables

Install the S9500 on a clean, dry, level surface. Identify the connectors and switches on the back panel and attach the cables.

Note: Check your router, hub, or computer documentation to determine if the device needs to be reconfigured or if the power supply needs to be switched off when you are connecting the new equipment to the LAN.



1. Connect one of the RJ-45 cables to the Trusted port and the LAN.

   Note: See “Cabling Requirements,” below.

2. Connect the other RJ-45 cable to the Untrusted port and the Internet.

   Note: See “Cabling Requirements,” below.

3. Connect the mini-DIN8 connector from the Power Adapter to the Power port, and plug the other end into an electrical outlet.

4. Optionally, you can connect a cable to the DMZ port and other equipment, such as a server or hub.

   Note: See “Cabling Requirements,” below.

5. Turn on the equipment connected to the S9500, if necessary. If the cables are connected correctly, the Link LED for each connection will be lit.

6. Insert your Netopia CD and follow the instructions to install an Internet browser and the Adobe Acrobat Reader, if you don’t already have them.

Note: If you are installing multiple S9500 devices, you should install and configure them one at a time; otherwise you will run into IP address conflicts.

Cabling Requirements

The Ethernet cables provided in your Netopia equipment package are straight-through cables. You can use straight-through cables to connect the ports of the S9500 to certain types of equipment; however, some ports with some equipment require a crossover cable. Refer to the tables below for the correct cable for your connection.

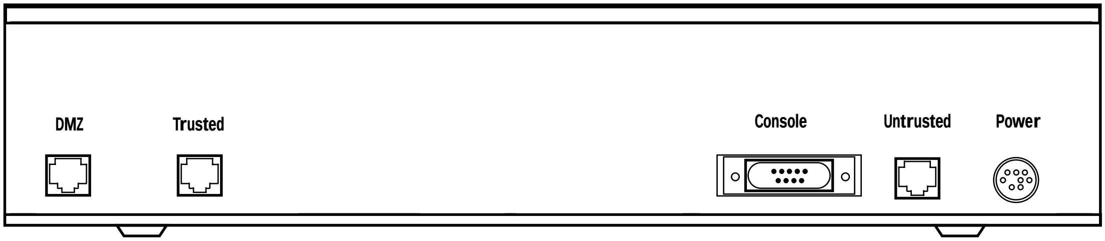
Use a Straight-Through cable to connect...	
this Port...	**to this Equipment.**
Untrusted port	Hub
Trusted port	Workstation Hub with the uplink switch enabled
DMZ port	Workstation Hub with the uplink switch enabled

Use a Crossover cable to connect...	
this Port...	**to this Equipment.**
Untrusted port	Workstation
Trusted port	Hub without an uplink switch
DMZ port	Hub without an uplink switch

Netopia S9500 Security Appliance Ports

The figure below displays the ports of the Netopia S9500 Security Appliance.

Netopia S9500 Security Appliance back panel



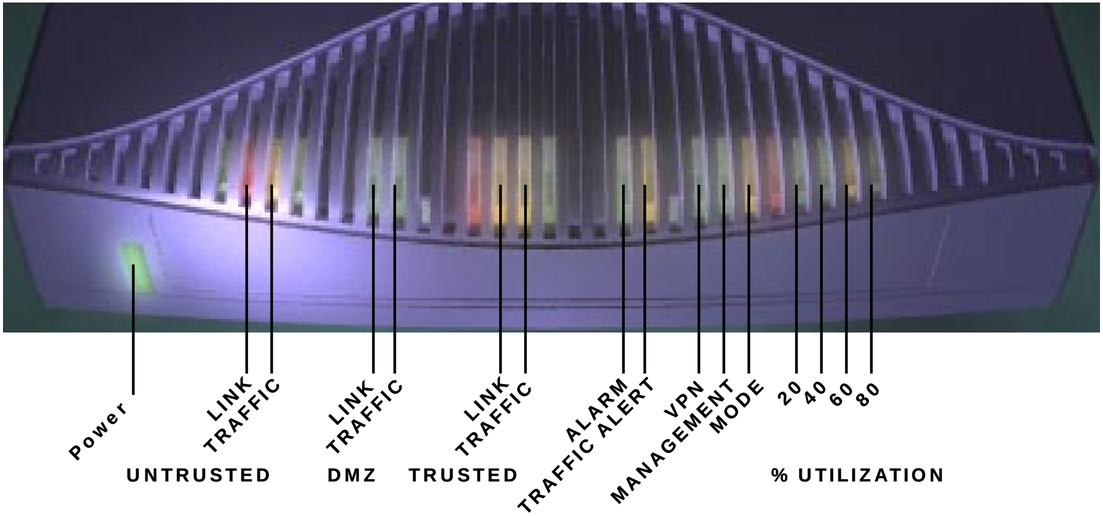
The following table describes all the Netopia S9500 Security Appliance ports.

Port	Description
Power port	A mini-DIN8 power adapter cable connection.
Untrusted port	An RJ-45 connector port labelled “Untrusted” for your Internet connection.
Console port	A DB-25 serial port connector for local configuration and administration.
Trusted port	An RJ-45 connector port labelled “Trusted” for your LAN connection.
DMZ port	An RJ-45 connector port labelled “DMZ” for other connections.

Netopia S9500 Security Appliance Status Lights

The figure below represents the Netopia S9500 status light (LED) panel.

Netopia S9500 Security Appliance front panel



The following table summarizes the meaning of the various LED states and colors:

The LED	Meaning
Power is solid **green**.	Power is on.
Untrusted Link is solid **green**.	Untrusted port is connected to an active device.
Untrusted Link is blinking **red**.	Untrusted network has experienced a collision.
Untrusted Traffic is blinking **yellow**.	Activity on Untrusted port
DMZ Link is solid **green**.	DMZ port is connected to an active device.
DMZ Link is blinking **red**.	DMZ network has experienced a collision.
DMZ Traffic is blinking **yellow**.	Activity on DMZ port
Trusted Link is solid **green**.	Trusted port is connected to an active device.
Trusted Link is blinking **red**.	Trusted network has experienced a collision.
Trusted Traffic is blinking **yellow**.	Activity on Trusted port
Alarm is solid **red**.	Alarm has occurred.
Traffic Alert is blinking **yellow**.	Traffic is heavy.
VPN is solid **green**.	VPN tunnel is established.
Management is solid **green**.	S9500 is managed via the console.
Management is blinking **green**.	S9500 is managed via the Web browser.
Mode is solid **green**.	Transparent mode is in effect.
Mode is unlit.	Network Address Translation mode is in effect.
20 is solid **green**.	CPU utilization is greater than 20%.
40 is solid **green**.	CPU utilization is greater than 40%.
60 is solid **yellow**.	CPU utilization is greater than 60%.
80 is solid **red**.	CPU utilization is greater than 80%.

Chapter 3

Configuration and Monitoring

The Netopia S9500 Security Appliance can be configured and monitored from a Web browser, a command line interface, an SNMP management program, or Netopia S9500 VPN Client software. This chapter will guide you through configuring the S9500 by using the Web Administration Tools of the Web browser.

For information on using SNMP, see Appendix A, “SNMP Support.”

For the commands for the command line interface, see Appendix B, “Command Line Interface.”

For information on Netopia S9500 VPN Client software, see the *Netopia-Remote Software IPSec Client Reference Guide* included on the Netopia CD.

This chapter covers the following topics:

- “Accessing the S9500 via a Web browser” on page 3-11
- “Configuring the S9500” on page 3-14
- “Monitoring the S9500” on page 3-42

Accessing the S9500 via a Web browser

To access the S9500 via a Web browser, you must have:

- Netscape Communicator V4.0 or later, or Microsoft Internet Explorer V4.01 or later
- a TCP/IP network connection to the S9500

If you have not configured the administration IP of the S9500, see the Getting Started Guide included in your Netopia folio for the Quick Configuration information.

To start a network connection from your computer to the S9500:

1. In the URL field of your Web browser, enter the IP address of the S9500. The Enter Network Password dialog box appears.
2. Type in the user name and the password.

   Note that the user name and password are case-sensitive.
3. Click **OK**. You are now logged on to the S9500, and the Netopia Web Administration page appears.

Web Administration Tools

The main menu of the Web interface consists of the Web Administration Tools. Laid out along the left-hand side of the page, there are four types of tools: System, Network, Lists, and Monitor. Beneath each of these tools are buttons that offer the utilities listed below.

System

The System tools are Configure and Admin.

Configure. Configure allows you to:

- set device options regarding the firewall, user, and authentication
- perform system updates
- define the IP address for each port
- set URL filtering and route tables.

The Configuration page has these tabs:

- General
- Interface
- Authen.
- URL Filtering
- Route Table

Admin. Admin allows you to set system administration options, such as:

- user name
- password
- e-mail alert
- sys log settings.

The Admin page has these tabs:

- Admin
- Sys log

Network

The Network tools are Policy, VPN, and Virtual IP.

Policy. Policy allows you to define policies to permit, deny, encrypt, authenticate, and shape traffic.

The Access Policies page has these tabs:

- Incoming
- Outgoing
- To DMZ
- From DMZ

VPN. VPN allows you to create a virtual private network.

The VPN Lists page has these tabs:

- Autokey IKE
- Manual Key

Virtual IP. Virtual IP allows you to configure virtual IP addresses. This utility is available only in NAT mode.

The Virtual IP page has these tabs:

- Virtual IP1
- Virtual IP2
- IP Mapping
- Dynamic IP

Lists

The Lists tools are Address, Service, Schedule, and Users.

Address. Address allows you to define IP addresses, subnets, and networks with user-defined names.

The Address page has these tabs:

- Trusted
- Untrusted
- DMZ

Service. Service allows you to view and define the services available for use in a policy.

The Service page has these tabs:

- Predefined
- Custom

Schedule. Schedule allows you to define schedules for use in a policy.

Users. Users allows you to define user names and passwords from an internal user database.

The Users page has the Define Users tab.

Monitor

The Monitor tools are Traffic, Counters, Alarm, and Log.

Traffic. Traffic allows you to view traffic information for each encrypt policy and bandwidth usage for each interface.

The Traffic page has these tabs:

- Policy
- Interface

Counters. Counters allows you to view graphs of bandwidth usage for each policy, if you enabled counting in the policy. The graphs can be displayed by last 60 seconds, minutes, hours, days, or months.

Alarm. Alarm allows you to view information for each policy for which you set alarm thresholds.

Log. Log allows you to view log details for each policy for which you enabled logging and to view system events.

The Log page has these tabs:

- Traffic Log
- Event Log

Central Display

The Central Display is the area of the screen where the tools and utilities list information and provide options for you to configure. These displays generally link to their related screens through action buttons in the lower left-hand corner of the screen.

Help

At any time, you can click the circled question mark in the upper right-hand corner of the screen to access on-line help.

Configuring the S9500

To configure the S9500, you can use these utilities:

- Address Book Setup (page 3-14)
- Service Book Setup (page 3-16)
- Schedule Book Setup (page 3-17)
- Policy Configuration (page 3-18)
- System Configuration (page 3-22)
- Interface Configuration (page 3-24)
- Authentication Configuration (page 3-26)
- URL Filtering Configuration (page 3-27)
- Route Table Configuration (page 3-28)
- Administrative Configuration (page 3-29)
- Syslog Configuration (page 3-30)
- VPN Configuration (page 3-31)
- IP Configuration (page 3-37)
- User Configuration (page 3-40)

Note: Most of the configurations outlined in this chapter take effect on a real-time basis as soon as you click the OK or Apply button. Some configurations require an equipment reboot; a dialog box will appear when rebooting is necessary.

Address Book Setup

Before you can set up any of the other S9500 firewall features, you need to define the Address Book. The Address Book contains the IP addresses of hosts that can have their traffic allowed, blocked, encrypted, or user-authenticated.

Note: The IP address 0.0.0.0 is predefined for all inside and all outside traffic.

View the Address Book

1. From the Web browser, in the Web Administration Tools menu, click the **Lists: Address** button. The Address Book page with Trusted, Untrusted, and DMZ tabs appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labeled “Trusted.” These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labeled “Untrusted.” These entries appear in red on your screen. DMZ addresses are individual IP addresses or subnets located behind the port labeled “DMZ.” These entries appear in a rust color on your screen.

   Individual hosts will have only a single IP address defined and will be represented with a single computer icon. Networks will have an IP address along with a subnet mask and will be represented with multiple computer icons.

2. Click a tab to view the addresses defined for the Trusted, Untrusted, or DMZ port.

Add an address or range of addresses

1. In the Address Book page, click the tab for the port you want to add an address to.
2. Click **New Address**. The Address Configuration page appears. Enter the information into these fields:

Field	Information
Address Name:	The name that will appear in the configuration window. Choose a descriptive name to help you easily identify the address. The name must be unique and is limited to 20 characters.
IP Address:	The IP address of the computer.
NetMask:	The subnet mask of the computer. The subnet mask, in combination with the IP address, can specify a range of addresses. For example, for the IP address 201.2.3.4, a subnet mask of 255.255.255.0 specifies a range of addresses from 201.2.3.0 to 201.2.3.255. On the other hand, for an IP address 201.2.3.4, a subnet mask of 255.255.255.255 specifies just 201.2.3.4.
Comment:	Any additional information is limited to 30 characters.
Location:	The location of the IP address relative to the S9500 port. This field automatically defaults to Trusted, Untrusted, or DMZ depending upon which tab you chose to add the address to originally, on the Address Book page.

Click **OK** to add the address.

Modify an existing address entry

1. In the Address Book page, click a tab to choose the Trusted, Untrusted, or DMZ port.
2. In the Configure column, click **Edit** for the address that you want to modify. The Address Configuration page appears.
3. Enter the new address information in the fields.

   Note: Remember that the address name must be unique. Further, once an address has been defined and referenced by a policy, you can change the address name but not its port type. To change its port type, you must first modify the underlying policy.

   Click **OK** to save the new address information.

Remove an existing address entry

1. In the Address Book page, click a tab to choose the Trusted, Untrusted, or DMZ port.
2. In the Configure column, click **Remove** for the address that you want to delete.

   Note: Addresses referenced by a policy cannot be removed until they are removed from the underlying policy.

Service Book Setup

In addition to addresses, every policy has a service associated with it. Services are IP traffic for which protocol standards exist. Each service has a port number associated with it, where the policy will accept a request for that service. Over 30 popular services such as HTTP, SNMP, and FTP have been predefined.

View the Service Book

1. From the Web browser, in the Web Administration Tools menu, click the **Lists: Service** button. The Service Book page with Predefined and Custom tabs appears.

   The Predefined services are color-coded to represent Remote, Email, Info Seeking, Security, and Other.

   - Remote includes various remote connection utilities such as FTP, RLOGIN, and Telnet.
   - Email includes services such as POP3 and Mail.
   - Info Seeking includes information search engines such as HTTP, gopher, and DNS.
   - Security includes services such as SHTTP.
   - Other includes miscellaneous utilities such as ICMP, SNMP, TCP-ANY, and SYSLOG.

   The Custom services are those you define by adding new services.
2. Select either tab to view the available services.

Add a service

1. In the Service Book page, select the Custom tab.
2. Click **New Service** in the lower left-hand corner of the screen, and the Service Configuration page appears. Enter the information into these fields:

Field	Information
Service Name:	A name to define the new service. This name will be used in policies that include this service.
Source Port:	Range of internal port numbers valid for that service.
Destination Port:	Range of external port numbers that will receive the service request.
Transport:	The protocol used by the service: TCP, UDP, or Other for a pre-defined service's number.
Reverse / Ack:	The confirmation method: reverse communication or acknowledged flag.

Click **OK** to save the addition.

Edit an existing service

Note: You can edit or delete existing Custom service entries, but you cannot edit or delete any Predefined service entries.

1. In the Service Book page, click the Custom tab.
2. In the Configure column, click **Edit** for the service that you want to modify. The Service Configuration page appears.
3. Enter the new service information in the fields. Click **OK** to save the new service information.

Remove an existing service

Note: You can edit or delete existing Custom service entries, but you cannot edit or delete any Predefined service entries.

1. In the Service Book page, click the Custom tab.
2. In the Configure column, click **Remove** for the service that you want to delete.

Schedule Book Setup

In addition to addresses and services, every policy has a schedule associated with it.

View the Schedule Book

From the Web browser, in the Web Administration Tools menu, click the **Lists: Schedule** button. The Schedule Book page appears, displaying a table of defined schedules.

Add a schedule

In the Schedule Book page, click **New Schedule**. The Schedule Configuration page appears. Enter the information into these fields:

Field	Information
Schedule Name:	The name that will appear in the configuration window. Choose a descriptive name to help you identify the schedule. The name must be unique and is limited to 20 characters.
Comment:	Any additional information limited to 30 characters.
Recurring: or **Once:**	The frequency of the schedule: recurring or once.
Start Date and Time: **Stop Date and Time:**	Recurring: When the schedule starts and ends in a weekly period. Both start and stop times must be entered to be configured. You can specify up to two time periods within the same day. Once: When the schedule starts and ends. Both start and stop times must be entered to be configured.

Click **OK** to add the schedule.

Modify an existing schedule

1. In the Schedule page, in the Configure column, click **Edit** for the schedule that you want to modify. The Schedule Configuration page appears.
2. Enter the new schedule information in the fields. Click **OK** to save the new schedule information.

Remove an existing schedule

In the Schedule page, in the Configure column, click **Remove** for the schedule that you want to delete.

Note: Schedules referenced by a policy cannot be removed until the underlying policy is removed.

Policy Configuration

Using the Address Book, Service Book, and Schedules you have defined, you can now define policies that allow the denial, acceptance, encryption, and authentication of incoming and outgoing connections to Trusted, Untrusted, To DMZ, and From DMZ servers.

All security entries on the S9500 are policies. The action of the policy can be a simple firewall rule such as permit or deny, which allows you to determine what traffic passes through the firewall based on IP session details. Policies can also protect the Trusted network from outsider attacks, such as the scanning of Trusted hosts, and monitor traffic attempting to cross your firewall. For example, you might want to restrict a particular subnet’s access to the Internet. You can use policies to control packet flows based on criteria such as the IP source or destination address range, TCP ports, UDP responses, Internet Control Message Protocol (ICMP) responses, and TCP responses.

Further, policies can define connections that must be encrypted, thus forming a Virtual Private Network (VPN). You can define policies that specify what services should be permitted, denied, encrypted, authenticated, logged, counted, or trigger an alarm. With policies enabled, you also can view counters, logs, and alarms.

In the Web browser, the following icons are used to identify policies:

✓	Permit	▦	Log
⊗	Deny	⏳	Count
🔓	Encrypt disabled	🚨	Alarm
🔒	Encrypt enabled	⊤	Traffic
👤	Authenticate	🕒	Schedule

Define a policy

1. From the Web browser, in the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page, with the Incoming, Outgoing, To DMZ, and From DMZ tabs, appears.

2. Click the tab for the port you want to create a policy for. Click **New Policy** in the lower left-hand corner. The Policy Configuration page appears. Enter the information in these fields:

Field	Information
Source Address:	Choose an address from the drop-down list for the host or network generating the connection. These are addresses you have already defined in the Address Book. For more information on the Address Book, see "Address Book Setup" on page 3-14.
Destination Address:	Choose an address from the drop-down list for the server receiving the connection request. These are addresses you have already defined in the Address Book. For more information on the Address Book, see "Address Book Setup" on page 3-14.
Service:	Choose a service from the drop-down list for the type of connection to be established. Services define the type of traffic. Core Internet services are predefined in the Service Book, or you can define custom services. For more information on the Service Book, see "Service Book Setup" on page 3-16.

Action:	Choose **Permit**, **Deny**, **Encrypt**, or **Authenticate** from the drop-down list. The S9500 will apply the action selected for this policy against traffic that matches the first three criteria: Source Address, Destination Address, and Service.
VPN Tunnel:	If the Action is not Encrypt, then leave **None** as the default for this field. If the Action is Encrypt, then select the appropriate VPN tunnel that matches the source and destination. For more information on VPN tunnels, see "VPN Configuration" on page 3-31.
Logging:	Select **Enable** to have the S9500 log all connections for this policy. You can view a log of connections to which this access policy was applied. For more information on logging, see "Logs" on page 3-44.
Counting:	Select **Enable** to have the S9500 count the total number of bytes for this policy and record the information in historical graphs. You can then view the graphs. For more details, see "Counters" on page 3-43.
Alarm Threshold:	Counting must be enabled to configure alarm thresholds. In the **Alarm Threshold** fields, enter the number of bytes per second, the number of bytes per minute, or both. **Note:** You can only enter integer values in the **Alarm Threshold** fields. A value of 0 indicates that the alarm has been disabled. If the value is greater than 0, the alarm is enabled, and you can view a log of alarms. For more details, see "Alarms" on page 3-43.
Schedule:	If you would like this policy enforced at all times, select **None** from the drop-down list. If you would like this policy enforced only during certain times, select a schedule from the drop-down list. These are schedules you have already defined in the Schedule Book. For more information on schedules, see "Schedule Book Setup" on page 3-17. **Note:** Policies will appear in green when they are not being enforced.

Traffic Shaping:	If this function is enabled, all traffic corresponding to this policy will be controlled and shaped according to these parameters:	
	Guaranteed Bandwidth:	Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management/ shaping mechanism.
	Maximum Bandwidth:	Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be dropped. **Note:** Rates less then 10 kbps should not be used. Rates below this threshold will lead to dropped packets and excessive retries that defeat the purpose of traffic management.
	Traffic Priority:	Traffic with higher priority will be passed first, and lower priority traffic will be passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.

Click **OK** to add the policy.

View or modify a policy

1. From the Web browser, in the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Incoming, Outgoing, From DMZ, or To DMZ policy tab to view those policies.
3. In the Configure column, click **Detail** for the policy that you want to change. The Policy Configuration page appears.
4. Specify the new information for the policy. Click **OK** to save the changes.

Remove a policy

1. From the Web browser, in the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Incoming, Outgoing, From DMZ, or To DMZ policy tab.
3. In the Configure column, click **Remove** for the policy that you want to delete. A System Message window will ask for user confirmation to proceed with the deletion. Click **OK**.

Arrange policies

All attempted access is checked against the policies beginning with the first policy listed on the Access Policies page and moving through the list. Action is taken on the first matching policy. Policies should be ordered from specific to general.

1. From the Web browser, in the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Incoming, Outgoing, From DMZ, or To DMZ policy tab.
3. Select a policy and click the up or down arrows to move the policy up or down.

   Note: Scheduled policies will be green when they are not being enforced at that moment.

System Configuration

You can view information on your S9500 and configure some of its system settings in the General Configuration page. The information you can view includes the Operation Mode and the Software Version. The settings you can configure include the DNS IP address, firewall settings, and clock synchronization.

From the Web browser, in the Web Administration Tools, click the **System: Configure** button. The Configuration page appears, with the General, Interface, Authen., URL Filtering, and Route Table tabs. Select the General tab.

System Information

In the General Configuration page, you can see which mode your S9500 is operating in. The two possible modes are Transparent and Network Address Translation.

- Transparent mode does not require any changes to routers or hosts at the time of installation and the S9500 is invisible.
- Network Address Translation mode will hide all Trusted IP addresses with all IP addresses appearing as one IP address. In this mode, the status of the DMZ port also is reported.

You can also see the software version running on your S9500 and its serial number.

Software Update

The S9500's firmware/software can be upgraded by using your Web browser to upload the latest release to your S9500 device. The latest firmware can be downloaded from the Netopia Web site. Once the upgrade is downloaded and saved to your administration workstation, return to the General Configuration page.

1. Click the **Browse** button next to the **Software Update** field.
2. Find the location of the new firmware on your computer's storage area, and select the new firmware.
3. Click the **Save and Reset** button in the lower right-hand corner of the General Configuration page.
4. The S9500 will reboot, and then you can reconnect to it through the Web browser.

DNS IP Address

This field's default value of 0.0.0.0 implies that the DNS address is defined in each host. If all DNS requests passing through the S9500 should go to a specified address of the DNS server, enter that address in this field.

Firewall Settings

The S9500 is capable of detecting access based on the following features:

- Detect SYN Attack: SYN Attacks occur when the connecting host continuously sends TCP syn requests without the corresponding ack response. The S9500 prevents syn packets without ack responses when this option is selected.

- Detect Tear Drop Attack: Tear Drop Attacks occur when TCP packets overlap, rendering Windows 95 machines dead. The S9500 intercepts these illegal connection requests, shielding valuable corporate computing resources on the internal network, when this option is selected.
- Detect IP Spoofing Attack: Spoofing attacks occur when unauthorized agents attempt to bypass the firewall security by imitating valid client IP addresses. The S9500 invalidates these false IP address connections when this option is selected.
- Detect Ping of Death Attack: The TCP/IP specification requires a specific packet size for datagrams being transmitted. Many ping implementations allow the user to specify a larger packet size if desired, which can trigger a range of adverse system reactions including crashing, freezing, and rebooting. The S9500 can be programmed to detect and reject such oversized and irregular packet sizes when this option is selected.
- Default Packet Deny: The S9500 denies all traffic not specifically allowed by a defined policy when this option is selected. Disabling this option would allow all traffic that is not denied by a policy. This could be useful for other non-network protocols that may be required for other services.
- Filter IP Source Route Option: IP header information has an option to contain routing information that may specify a different source than the header source. Source Route Option can allow an attacker to enter a network with a fake IP address and have data sent back to the real address. The S9500 blocks all IP traffic that uses Source Route Option when this option is selected.

Synchronize System Clock:

The S9500's system clock should be synchronized with real time so the logs will reflect the actual time of events. To set the system clock of the S9500, select the **Synchronize system clock with this client** option, and click **Apply**.

Note: If you are managing the S9500 remotely across time zones, the time of the S9500 will be the same as the administration workstation.

Download and Upload System Configuration

The S9500 configuration can be downloaded and uploaded. The configuration contains all the device's general, admin, interface, policy, user-defined services, and users database settings. This data can be used to configure other devices or in case of failure, to configure a new device.

1. From the Web browser, in the Web Administration Tools, click the **System: Admin** button. The Administration page appears, with the Admin. and Sys Log tabs. Select the Admin. tab.
2. Click **Download Configuration** in the lower left-hand corner of the screen to start the download process and save the file to the administration workstation. Follow the Web browser instructions to save the file.

To upload the configuration into a S9500 device:

1. From the Web browser, in the Web Administration Tools, click the **System: Admin** button. The Administration page appears, with the Admin. and Sys Log tabs. Select the Admin. tab.
2. Click the **Browse** button next to the **Configure Script Upload** field in the middle of the page. Follow the Web browser instructions to locate the file and open it.
3. The S9500 will upload the file and reset automatically. If the administration IP is different, then you will have to reconnect to the new IP address.

Interface Configuration

The S9500 has four interfaces: Web Management, Trusted, Untrusted, and DMZ. Once those interfaces are configured, that configuration is reported in the Interface Configuration page, where you can also change the configuration.

The S9500 ships from the factory in Transparent mode with only the Trusted and Untrusted interfaces operational. The Web Management interface becomes operational when you configure the S9500 VPN Client software for central management (see the *Netopia-Remote Software IPSec Client Reference Guide* included on the Netopia CD for more information). Both the Web Management interface and the DMZ interface become operational when you configure the S9500 for Network Address Translation mode (see “Network Address Translation mode,” below).

To access the Interface Configuration page, from the Web browser, in the Web Administration Tools, click the System: Configure button. The Configuration page appears, with the General, Interface, Authen., URL Filtering, and Route Table tabs. Select the Interface tab.

Transparent mode

Transparent mode allows users to access the Internet while denying access from the Internet. This mode is the easiest to install as it requires no changes to network addresses or topology. In Transparent mode, the Trusted and Untrusted ports have IP addresses 0.0.0.0. See the Getting Started Guide included in your Netopia folio for configuration information on the Transparent mode.

Network Address Translation mode

The Network Address Translation (NAT) mode enables NAT on your local network. NAT provides anonymity to machines on the corporate LAN by connecting the entire network to the Internet using a few registered IP addresses. Also, if an IP address range has been arbitrarily selected on your LAN, it is possible that those IP addresses are invalid and consequently will not be able to access some Internet sites that have been assigned that same IP address range. For example, if the address range 199.2.23.1 through 199.2.23.255 is used on the LAN, a Web server on the Internet with the address of 199.2.23.20 will not be accessible.

Therefore, if your LAN is using IP addresses that have not been assigned by an ISP, it is a good idea to allocate a special IP address range for this purpose. The following IP address ranges are reserved for private IP networks and do not get routed on the Internet:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

NAT supports ICMP, UDP and TCP-based applications.

To enable NAT:

1. From the Web browser, in the Web Administration Tools, click the **System: Configure** button. The Configuration page appears. Click the Interface tab. The Interface page appears.

2. Enter the following information:

Field	Information
Web Management Interface System IP:	The IP address of the S9500 for central management.
Port:	The number of the port that will supply HTTP configuration requests to the S9500. The default is 80, but you can change this to any secret number between 1024 to 32767 to discourage unauthorized access and modifications to the configuration of your S9500. If you change the port number, you need to enter it in your browser with the IP address; for example, http://172.168.10.157:port-number.
Trusted Interface (Physical Address):	The unique address of the Ethernet network interface for the Trusted port. The MAC value is reported for information purposes. The current status of the interface is also reported. This field is not modifiable.
(Trusted) Inside IP:	The IP address used on the Trusted side. If the internal network consists of only one subnet, then the default gateway of all computers must be set up to point to the (Trusted) NAT Inside IP address. If the internal network consists of multiple subnets, then the default gateway of the internal router must be set up to point to the (Trust) NAT Inside IP address.
(Trusted) Inside Netmask:	The subnet mask of the inside IP addresses.
(Trusted) Default Gateway IP:	The IP address of the default gateway for the Trusted interface which is generally the IP address of the router. A Default Gateway IP of 0.0.0.0 indicates that the S9500 can transfer packets to only one subnet.
(Trusted) Traffic Bandwidth:	The actual line speed in kilobits per second (kbps).
Untrusted Interface (Physical Address):	The unique address of the Ethernet network interface for the Untrusted port. The MAC value is reported for information purposes. The current status of the interface is also reported. This field is not modifiable.
(Untrusted) Outside IP:	A valid IP address that will be used by Untrusted hosts to refer to the Trusted port interface.

(Untrusted) Outside Netmask:	The subnet mask of the outside IP address.
(Untrusted) Default Gateway IP:	The IP address of the default gateway for the Untrusted interface which is generally the IP address of the internal router.
(Untrusted) Traffic Bandwidth:	The actual line speed in kilobits per second (kbps).
DMZ Interface (Physical Address):	The unique address of the Ethernet network interface for the DMZ port. The MAC value is reported for information purposes. The current status of the interface is also reported. This field is not modifiable.
DMZ IP:	A valid IP address that will be forwarded to the DMZ hosts to refer to the Trusted port interface.
(DMZ) Netmask:	The subnet mask of the DMZ IP address.
(DMZ) Traffic Bandwidth:	The actual line speed in kilobits per second (kbps).

Note: There is no Default Gateway IP address for the DMZ port because the S9500 supports a DMZ that has only one subnet.

3. Click **Save and Reset** to have the new settings take effect and to restart your S9500.

Authentication Configuration

The S9500 policies can support user authentication before network access is allowed. The S9500 supports a built-in user database or can be linked to a Radius Server. The Radius Server must be located on the Trusted network. You can set up authentication in the Authentication (Authen.) Configuration page.

From the Web browser, in the Web Administration Tools, click the **System: Configure** button. The Configuration page appears, with the General, Interface, Authen., URL Filtering, and Route Table tabs. Select the Authen. tab.

User Idle Timeout

This setting determines how much time of user inactivity must elapse before the S9500 will end the user session. The value can be from 0 to 65,000 minutes. A value of 0 would determine that the S9500 never ends an idle session. The default is 10 and is highly recommended since shorter time intervals may be bothersome to normal user usage and longer intervals may leave the network open to unwanted access.

User Idle Timeout is the same no matter which database is used.

Authentication Method Settings

You can select the Built-in User Database or Radius Server to provide information for user authentication.

Built-in User Database. The S9500 built-in user database can be used if an external Radius Server is not available. The user database can support up to 1,500 entries which are entered in the User Lists page. See “User Configuration” on page 3-40 for more information.

Radius Server. If authentication will be confirmed from a Radius server, the Radius server must be located on the Trusted network, and you must enter the following information:

Field	Information
Server IP:	The IP address of the Radius server.
Shared Secret:	The shared secret must be the same as defined in the Radius setup. See your Radius documentation for details.

Authentication Notes

- If a policy is for a subnet of IP addresses (for example, inside any), each IP address will have to authenticate. If one of the hosts supports multiple user accounts (for example, Unix host running Telnet), then once one user authenticates all users from that host could pass through the device without authentication since the S9500 records the IP address only.
- As most Web browsers cache user name and password, it will authenticate the user again with the S9500 and reinitiate the timeout value.

URL Filtering Configuration

The S9500 can block access to different sites based upon their URLs. The S9500 has created a direct link to NetPartners' WebSense URL blocking software. WebSense is ranked as one of the top Internet access management tools. Additional information about WebSense can be found at http://www.websense.com. WebSense needs to be installed on a separate NT workstation or server. To set up URL filtering, go to the URL Filtering Configuration page.

From the Web browser, in the Web Administration Tools, click the **System: Configure** button. The Configuration page appears, with the General, Interface, Authen., URL Filtering, and Route Table tabs. Select the URL Filtering tab.

To configure URL filtering:

1. Select the **Enable URL Filtering via WebSense Server** option to enable this feature and enter the following information:

Field	Information
WebSense Server IP:	The IP address of the computer running the WebSense server. The WebSense server must be located on the Trusted side of the S9500 device.
WebSense Server Port:	The default port for WebSense is 15868. If you have changed the default port on the WebSense server you need to change it on the S9500 also. Please see your WebSense documentation for full details.

Communications Timeout:	The time interval, in seconds, that the S9500 will wait for a response from the WebSense filter. If WebSense does not respond within the time interval, the S9500 will ultimately block the request.
Current Server Status:	The status of the WebSense server. This field is not modifiable.
URL Block Return Message:	The message the S9500 will return to the user after blocking the site. You can enter a custom message of up to 220 characters.

2. Click **Apply** to save the changes.

   Note: WebSense requires that its service be stopped and restarted before any changes in options will take affect. Please refer to WebSense documentation for WebSense configuration.

Route Table Configuration

The Route Table provides the S9500 with information to direct data to different subnets, so the S9500 can support complex networks. Defined routes are required when multiple Internet connections are installed and if multiple subnets are used on the Trusted network.

From the Web browser, in the Web Administration Tools, click the **System: Configure** button. The Configuration page appears, with the General, Interface, Authen., URL Filtering, and Route Table tabs. Select the Route Table tab.

The Route Table tab in the Configuration page provides a read-only summary of static routes defined by the S9500 if any of the three interfaces have been defined. These static routes provide proper routing for packets passing through the S9500 unit. The route tables are automatically configured once the Trusted, Untrusted, and DMZ interfaces are defined. If the Trusted interface will have more than one subnet or if the Trusted and Untrusted network has more than one router then it is necessary to define static routes.

Define static routes

1. From the Static Route Table Configuration page, click **New Entry** in the lower left-hand corner of the screen. The Route Table Configuration page appears.
2. Enter the following information:

Field	Information
Network Address:	The IP address of the internal server.
Network NetMask:	The subnet mask of the internal network.
Gateway IP Address:	The IP address of the router that will forward the traffic on the same subnet.

Interface:	The interface the network is connected to, either the Trusted or Untrusted.
Metric:	A predefined parameter that defines the priority of the route. All predefined metrics are given a value of 0 and any user-defined routes are given a value 1. This value is not user-definable.

3. Click **OK** to add the new route table configuration.

Modify an existing route table

1. From the Static Route Table Configuration page, in the Configure column, click **Edit** for the entry that you want to modify. The Route Table Configuration page appears.
2. Enter the new information in the fields, and click **OK** to save the changes.

Remove an existing route table

1. From the Static Route Table Configuration page, in the Configure column, click **Remove** for the entry that you want to delete.
2. A System Message window will ask for user confirmation to proceed with the deletion. Click **OK**.

Administrative Configuration

You can restrict user access to the administration of the S9500 with these options:

- Admin Login Name and Password
- Administration from One or Multiple Addresses
- Administration through the Untrusted Port
- E-Mail Alert Notification

From the Web browser, in the Web Administration Tools, click the **System: Admin** button. The Administration page appears, with the Admin. and Sys Log tabs. Select the Admin. tab.

Modify the Admin Login Name and Password

1. In the Admin Administration page, change the login name by entering a new login name in the **Admin Login Name** field. You can then use the new user name with the old password. You can use only one user name per S9500 device.
2. Change the password by entering the current password in the **Old Password** field, and then entering the new password in the **New Password** and **Confirm New Password** fields.
3. Click **Apply** to have your changes take effect.

Restrict Administration to One Address

1. In the Admin Administration page, enter the specific IP address in the **Admin Client IP** field and its subnet mask in the **NetMask** field. The default address, 0.0.0.0, allows administration from any address.

   Note: If you are using the Web interface to administer the S9500 and enter an invalid IP address and click **OK**, the screen will revert back to a 0.0.0.0 default IP address.

2. Click **Apply** to have your changes take effect.

Administration through the Untrusted Port

You can configure the S9500 to allow administration of the device from both the Trusted and Untrusted side, or just from the Trusted side. To maintain the highest level of security, you should allow only Trusted network access to the unit, restricting administrative access from Untrusted port.

Note: It is not possible to administrate the S9500 from the DMZ port.

1. In the Admin Administration page, to enable administration through the Untrusted port, select **Enable Untrusted Side Logon**.

   Unselecting this option allows administration through the Trusted port only.

2. Click **Apply** to have your changes take effect.

E-mail Alert Notification

The S9500 can alert you via e-mail whenever an alarm is triggered. For more information on the Alarm feature, see “Alarms” on page 3-43.

1. In the Admin Administration page, select **Enable E-Mail Alert Notification** and enter the following information:

Field	Information
SMTP Server IP:	The IP address of the SMTP mail server. SMTP server names are not supported at this time.
E-Mail Address 1:	The e-mail address of the first user to be notified.
E-Mail Address 2:	The e-mail address of the second user to be notified.

2. Click **Apply** to have your changes take effect.

Syslog Configuration

The S9500 generates syslog messages for system events, such as security alerts and system events. Messages are sent to the syslog host over UDP. Syslog messages may be used by the syslog host to create e-mail alerts and log files, or the messages may be displayed on the console of a designated host using UNIX syslog conventions.

Your Syslog server must be located on the Trusted side of the S9500.

1. From the Web browser, in the Web Administration Tools menu, click the **System: Admin** button. The Administration page appears, with the Admin. and Sys Log tabs. Select the Sys Log tab.

2. To enable syslog, select **Enable Syslog Messages** and enter the following information:

Field	Information
Syslog Host IP Address:	The IP address of the Syslog host. The Syslog host must be located on the Trusted side of the S9500.
Syslog Host Port:	The port number that the Syslog UDP packets will be sent on. The default is 514.
Security Facility:	The level of security facility. The default is Local0.
Facility:	The level of facility. The default is Local0.
Only log messages with a priority level of "x" or higher:	The minimum priority level of a message to be sent. Select one of the following priority levels:
EMERGENCY	System unusable message
ALERT	Take immediate action
CRITICAL	Critical condition
ERROR	Error message
WARNING	Warning message
NOTICE	Normal but significant condition
INFO	Information message
DEBUG	Debug message

3. Click **Apply** to have your changes take effect.

The SYSLOG reports can also be customized through WebTrends for Firewalls and VPNs, an add-on for the Netopia S9500 Security Appliance. WebTrends manages, monitors, and reports on security issues and network traffic in real time. For more information, see the WebTrends CD included in your Netopia folio.

VPN Configuration

With a virtual private network (VPN) you can access the S9500 remotely. To support a VPN, the S9500 also must support encryption. So first you must set up an encryption policy and then you must set up a policy for VPN.

Encryption Policy Configuration

To set up an encryption policy, you have to define its VPN tunnel and both ends of the tunnel must be configured the same.

From the Web browser, in the Web Administration Tools menu, click the **Network: VPN** button. The VPN Lists page, with the Autokey IKE and Manual Key tabs, appears.

The S9500 supports two types of key methods for VPNs: Autokey IKE and Manual Key. Select a tab to create encryption with Autokey IKE or Manual Key.

Create an Autokey IKE VPN. Internet Key Exchange (IKE) provides a standard method to automatically negotiate keys between two security gateways; i.e., the S9500s. Autokey IKE will allow new keys to be generated after a set amount of time has passed or a certain threshold of traffic has been exchanged.

1. Click **New VPN Entry** in the lower left-hand corner of the screen. The IKE VPN Configuration page appears.
2. Enter the following information:

Field	Information
VPN Name:	The name to identify this VPN tunnel definition. Choose a descriptive name to help you identify the VPN tunnel. The name must be unique and is limited to 20 characters.
Gateway IP:	The IP address of the remote LAN S9500’s Untrusted interface or other IPSec device. Check the manufacturer’s documentation for the IP address.
Preshared Key:	The preshared Key. The Key may be up to 128 bytes long.
ESP-Encryption Algorithm:	The algorithm to use for encryption: ■ NULL ■ no encryption ■ 56bit DES-CBC ■ 3DES-CBC ■ 40bit DES-CBC.
ESP-Authentication Method:	The algorithm to use for authentication: ■ NULL ■ MD5 ■ SHA 1
Key Life Time:	The definition of how and at what threshold to rekey on. New keys will be generated whenever the lifetime of the old key is exceeded. Select time (seconds) or size (bytes) to rekey on and define the threshold. Selection of small values could lead to frequent rekeying, which could affect performance. The default is 3600 seconds, one hour.

3. Click **OK** to save.

Create a Manual Key VPN. Manual Key VPNs only use one key.

Note: Currently Netopia S9500 VPN Client software only supports Manual Key. Any VPNs defined for remote access must use Manual Keys.

1. Click **New VPN Entry** in the lower left-hand corner of the screen. The Manual Key VPN Configuration page appears.
2. Enter the following information:

Field	Information
VPN Name:	The name to identify this VPN tunnel definition. Choose a descriptive name to help you identify the VPN tunnel. The name must be unique and is limited to 20 characters.
Gateway IP:	The IP address of the remote LAN S9500's Untrusted interface. For information on remote client configuration, see "VPN and Remote Client" on page 3-36.
Security Index (Local and Remote):	A unique security index number that will distinguish a particular encrypted tunnel from the others being used at the same time. Only a HEX value greater than 3000 is accepted. The Local Security Index will serve as the other end's Remote Security Index and vice versa.
ESP-DES Algorithm:	The algorithm to use for encryption: ■ NULL ■ DES-CBC ■ 3DES-CBC ■ 40bit DES-CBC.
HEX Key:	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). For DES only the left-most value needs to be defined. For 3DES all three values must be defined. The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.

ESP-Authentication Algorithm:	The algorithm to use for authentication: ■ NULL ■ MD5 ■ SHA-1.
HEX Key:	A security key used as an encryption key for the algorithm specified. MD5 uses 16 bytes and SHA-1 uses 20 bytes. Each field of the key is 8 or 10 bytes long represented in HEX. (The key is 16 or 20 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.

3. Click **OK** to save the new entry.

VPN Policy Configuration

Once you have defined a VPN in an encryption policy, you must set up a policy for VPN.

1. From the Web browser, in the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page, with the Incoming, Outgoing, To DMZ, and From DMZ tabs, appears
2. Select the Outgoing Policy tab, and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.

   Note: VPN polices are only defined for Outgoing traffic. VPN policies assume bi-directional traffic and assume that the destination address can originate VPN sessions.

3. Enter the following information:

Field	Information
Source Address:	The address for the host or network generating the connection. Select an option from the drop-down list.
Destination Address:	The address for the server receiving the connection request. Select an option from the drop-down list.
Service:	The service for the type of connection to be established. Select an option from the drop-down list.
Action:	Encrypt.

Logging:	Enable (to have the S9500 log all connections for this policy).
VPN Tunnel:	The VPN tunnel defined in the encryption policy. See “Encryption Policy Configuration” on page 3-32. Select an option from the drop-down list.
Counting:	Enable (to have the S9500 count the total number of bytes for this policy and record the information in historical graphs).
Alarm Threshold:	The number of bytes per second, the number of bytes per minute, or both. A value of 0 indicates that the alarm has been disabled. **Note:** You can only enter integer values in the **Alarm Threshold** fields.
Schedule:	The schedule for enforcing this policy. “None” means the policy is always on. For scheduling information, see “Schedule Book Setup” on page 3-17. **Note:** Policies will appear in green when they are not being enforced.
Traffic Shaping:	The specifications for controlling and shaping traffic. The traffic shaping parameters include:
Guaranteed Bandwidth:	Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management/ shaping mechanism.
Maximum Bandwidth:	Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be dropped. **Note:** Rates less then 10 kbps should not be used. Rates below this threshold will lead to dropped packets and excessive retries that defeat the purpose of traffic management.
Traffic Priority:	Traffic with higher priority will be passed first, and lower priority traffic will be passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.

4. Click **OK** to add the VPN policy.

VPN and Remote Client

VPNs can be configured to operate with Netopia S9500 VPN Client software. VPNs for remote users are configured on a per user basis.

To configure the S9500 for VPN and a remote user, create a policy.

1. From the Web browser, in the Web Administration Tools menu, click the **Lists: Users** button. The User page, with the Users and Dialup Group tabs, appears. Select the Users tab.
2. Click **New User** in the lower left-hand corner of the screen. The User Configuration page appears.
3. Enter the following information:

Field	Information
User Name:	The name to be validated. The name must be unique and is limited to 20 characters.
type of user name: Authentication User or VPN Dialup User	VPN Dialup User.
User Group:	A dialup user group.
Security Index (Local):	The local security index for this dialup user.
Security Index (Remote):	The remote security index for this dialup user.
ESP-Encryption Algorithm:	The encryption algorithm to be used: ■ NULL ■ DES-CBC ■ 40bit DES-CBC.
Key:	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). For DES only the left-most value needs to be defined. For 3DES all three values must be defined. The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.

ESP-Authentication Algorithm:	The algorithm to use for authentication: ■ NULL ■ MD5 ■ SHA-1.
HEX Key:	A security key used as an encryption key for the algorithm specified. MD5 uses 16 bytes and SHA-1 uses 20 bytes. Each field of the key is 8 or 10 bytes long represented in HEX. (The key is 16 or 20 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.

4. Click **OK** to save the addition.

IP Configuration

The S9500 can be configured to respond to many different IP addresses on the Untrusted Interface. Virtual IP functionality allows the S9500 to map different services to different IP addresses. Mapped IP functionality allows for one-to-one mapping of internal hosts to the Untrusted Interface. Dynamic IP functionality allows the S9500 to use additional IP addresses for Network Address Translation (NAT).

Virtual IP

The S9500 can configure up to two Virtual IP addresses and up to six services for each Virtual IP. The two Virtual IP addresses can forward traffic to four different servers in the Trusted network.

Note: Use this feature with caution. If an attacker gains access to one of the internal servers then the whole network could be in jeopardy.

The Virtual IP feature provides the following advantages:

- Security: In a Network Address Translation (NAT) environment, host computers use non-routable IP addresses inside the firewall while maintaining full Internet connection and functionality. This feature gives network administrators flexibility to grow their networks without being constrained by the scarcity of legal IP addresses. In addition, NAT also provides better network security by hiding internal network topology and host information from the outside world.

  However, in order to maintain some Internet services (e.g., e-mail, POP3, ftp), a server with a legal IP address must be present to service the requests. Virtual IP allows you to map routable IP addresses to internal servers, therefore providing transparent connections for a NAT network to the Internet.
- Scalability: As Internet service demand increases, companies need to improve servers' performance in order to maintain the quality of their services. While upgrading the server to a larger, faster machine will

generally relieve the short-term pressures, the disruption to services and the prohibitive cost of upgrading quickly make this solution undesirable. Virtual IP allows growth without disruption.

- High Availability: With Virtual IP, servers can be assigned to the same IP address and mirrored to provide high availability for network services. Individual servers can also be taken off-line for maintenance without disruption.
- Reduction in capital cost: Multiple domains and web servers can be mapped to the same physical server, thus reducing the cost of computer equipment as well as the associated administration tasks.

To configure for Virtual IP:

1. From the Web browser, in the Web Administration Tools, click the **Network: Virtual IP** button. The Virtual IP page appears, with the Virtual IP 1, Virtual IP 2, IP Mapping, and Dynamic IP tabs. Select either of the Virtual IP tabs.
2. Click the link at the top of the page to configure that Virtual IP address. The Virtual IP Configuration page appears.
3. In the **Virtual IP Address** field, enter the legal IP address that will be mapped from the Untrusted interface to the Trusted or DMZ port, and click **OK**. The Virtual IP page reappears.

   Note: Setting the IP address to 0.0.0.0 or clicking the **Clear** button on the configuration page will clear the Virtual IP address.
4. Define the service to be mapped by clicking **New Service** in the lower left-hand corner of the Virtual IP page. The Virtual IP Service Configuration page appears.
5. Enter the following information:

Field	Information
Virtual Port:	The port that the service should be mapped to. You can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service:	The service that should be mapped to the port.
Server IP:	The IP address of the server on the Trusted or DMZ network.

6. Click **OK**. Up to six services per Virtual IP can be configured.

To remove an existing Virtual IP:

Note: The Virtual IP field is not editable or removable when there are existing policies using its definition.

1. From the Web browser, in the Web Administration Tools, click the **Network: Virtual IP** button. The Virtual IP page appears, with the Virtual IP 1, Virtual IP 2, IP Mapping, and Dynamic IP tabs.
2. Select either of the Virtual IP tabs, and click the link at the top of the page. The Virtual IP Configuration page appears.
3. Select the IP address and click **Clear** or enter 0.0.0.0 as the IP address.

Mapped IP

Mapped IP is a direct one-to-one map of an IP address. The S9500 can support up to 1000 entries. Each entry represents only one IP address. The S9500 will route IP addresses to the DMZ subnet if the DMZ has been defined. All other IP addresses will be mapped to the Trusted IP network or Trusted IP Gateway if defined.

Note: A policy must be defined allowing the mapped IP address to be assessed. No address book entry is required for Mapped IP. The Mapped IP address will automatically appear in the Policy Configuration Source selection pop-up window.

To enable Mapped IP:

1. From the Web browser, in the Web Administration Tools, click the **Network: Virtual IP** button. The Virtual IP page appears, with the Virtual IP 1, Virtual IP 2, IP Mapping, and Dynamic IP tabs. Select the IP Mapping tab.
2. Click **New Entry** in the lower left-hand corner of the screen. The IP Mapping Configuration page appears.
3. Enter the following information:

Field	Information
Untrusted IP Address:	The IP address that is being configured.
Network NetMask:	The subnet mask of the mapped address.
Map to IP Address:	The IP address of the host to receive mapped traffic.

4. Click **OK**.

Dynamic IP

Dynamic IP allocates an IP address for those applications (e.g., Rlogin) which it is necessary to use more than one IP address when the S9500 is in NAT mode. Configuring Dynamic IP creates an IP address pool that outgoing traffic can use for the IP source destination.

These configuration rules must be followed:

- IP addresses must be in the same subnet as the Untrusted interface and must be part of the assigned IP address from the Internet service provider (ISP).
- The S9500 can support up to 4 entries.
- Each entry can represent either a single IP address or a range of contiguous IP addresses with no more than 255 in a range.
- An IP address configured for Dynamic IP use cannot be used for Virtual IP or Mapped IP.

To enable Dynamic IP:

1. From the Web browser, in the Web Administration Tools, click the **Network: Virtual IP** button. The Virtual IP page appears, with the Virtual IP 1, Virtual IP 2, IP Mapping, and Dynamic IP tabs. Select the Dynamic IP tab.
2. Click **New Entry** in the lower left-hand corner of the screen. The IP Mapping Configuration page appears.

3. Enter the following information:

Field	Information
IP Address Range Low:	The first IP address that will serve as the lowest value of the Dynamic IP address range.
IP Address Range High:	The last IP address that will serve as the highest value of the Dynamic IP address range.

4. Click **OK**.

User Configuration

The S9500's Users List can either define users for authentication or for VPN access. Authentication uses one of two methods to authenticate users: internal database or external Radius server. Authentication allows you to verify a connection before establishing it. The client requesting the connection is required to provide a user name and password to prove his or her validity in accessing your network.

The authentication mechanism requires that the user respond to a prompt for a user name and password. Authentication can be done via HTTP (web browser), FTP, or Telnet. No client software is required, but users of Mail, Gopher, and other services need to authenticate first via a Web browser, Telnet or FTP session.

For example, users want to use Gopher, but the access policy requires authentication. They first open a Web browser and attempt to make a connection to the site they are trying to reach. As soon as the S9500 sees the packet, it will ask the users for authentication. Once they enter a user name and password that matches an entry in the Users List, they will be authenticated to pass through the S9500. That authentication lasts a default of 10 minutes when idle. Then the packet will be processed through the S9500. If you do not actually have an HTTP server at that IP, the Web browser will just spin. Either way, the user is now authenticated.

Once authenticated, users can proceed to make any other connection, be it FTP, Telnet, or whatever is allowed by the access policy. When a packet comes to the S9500, it will check to see that the user must authenticate in order to pass. It will then check its authentication cache table and see if this IP has already been authenticated and is currently enabled. If so, the S9500 will pass the packets without prompting. The user's IP will be removed from the authentication cache table after the idle timeout has been reached.

If you have selected the internal user database, follow the directions below. If you have selected an external server, see page 3-26.

To enter a new user in the internal user database:

1. From the Web browser, in the Web Administration Tools, click the **Lists: Users** button. The User Lists page appears, with the Users and Dialup Group tabs. Select the Users tab.
2. Click **New User** in the lower left-hand corner of the screen. The User Configuration page appears.
3. Enter the following information:

Field	Information
User Name:	The name to be validated. The name must be unique and is limited to 20 characters.
type of user name:	Authentication User or VPN Dialup User.

4. If you enabled **Authentication User**, skip to step 5. If you enabled **VPN Dialup User**, enter the following information:

Field	Information
User Group:	A dialup user group.
Security Index (Local):	The local security index for this dial up user.
Security Index (Remote):	The remote security index for this dial up user.
ESP-Encryption Algorithm:	The encryption algorithm to be used: ■ NULL ■ DES-CBC ■ 40bit DES-CBC.
Key:	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). For DES only the left-most value needs to be defined. For 3DES all three values must be defined. The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.
ESP-Authentication Algorithm:	The algorithm to use for authentication: ■ NULL ■ MD5 ■ SHA-1.
Key:	A security key used as an encryption key for the algorithm specified. MD5 uses 16 bytes and SHA-1 uses 20 bytes. Each field of the key is 8 or 10 bytes long represented in HEX. (The key is 16 or 20 characters long with two characters used to describe one byte in HEX). The value must be odd bit parity (the sum of the 8 bits must be odd). The S9500 will automatically change your key value to ensure the requirement.
Generated Key by Password:	A password to define the generation of the hex key. **Note:** The use of the password feature is a convenience and may lead to similar keys.

5. If you enabled **VPN Dialup User**, skip this step. If you enabled **Authentication User**, enter the following information:

Field	Information
Authentication Password:	The password for the user.
Confirm Password:	The password for the user.
Status:	Enable or Disable authentication.

6. Click **OK** to save the addition.

To modify an existing user entry:

1. From the User Lists page, in the Configure column, click **Edit** for the entry that you want to modify. The User Configuration page appears.
2. Enter the new information in the fields.
3. Click **OK** to save the changes.

To remove an existing user configuration:

1. From the User Lists page, in the Configure column, click **Remove** for the entry that you want to delete.
2. A System Message window will ask for user confirmation to proceed with the deletion. Click **OK**.

Monitoring the S9500

The S9500 helps you monitor your network traffic and connections activity to determine if there were any attempts to compromise the security of the network.

You can define network monitors and view the results for:

- Traffic
- Counters
- Alarm
- Log

Traffic Allocation

To view the policy traffic allocation:

1. From the Web browser, in the Web Administration Tools, click the **Monitor: Traffic** button. The Traffic Table page, with the Policy and Interface tabs, appears. Select the Policy tab.

   All policies with traffic shaping turned on will be shown on this table. Each policy is identified by source address, destination address, service type, priority, direction, and traffic setting.

   The **Direction** field indicates whether it is a policy from Trusted (T) to Untrusted (U), Trusted (T) to DMZ (D), Untrusted (U) to Virtual IP (V), or other combinations.

The **Traffic Setting** field shows the guaranteed rate in blue and the maximum rate in red. The ratio is proportional to its own maximum rate specified in the policy. Service has bi-directional traffic. The top arrow specifies the amount of forward traffic (i.e., from source address to destination address) in kilobits per second (kbps) and the bottom arrow specifies the amount of backward traffic (i.e., from destination address to source address) in kilobits per second (kbps).

2. Click **Update Now** to get the current information.

To view the interface traffic:

1. From the Web browser, in the Web Administration Tools, click the **Monitor: Traffic** button. The Traffic Table page, with the Policy and Interface tabs, appears. Select the Interface tab.

   This page shows the physical bandwidth, configured bandwidth, guaranteed bandwidth, and the total utilization bandwidth for the S9500's Trusted, Untrusted, and DMZ interfaces.

2. Click **Update Now** to get the current information.

Counters

You can view counters and save the information after you include the counters in a policy. See "Define a policy" on page 3-19 for information on including counters in a policy.

To view and save information on counters:

1. From the Web browser, in the Web Administration Tools, click the **Monitor: Counters** button. The Counter Table page appears.
2. In the Details column, click **View Count Details** for the counter you want to view. The Counter Details page appears.
3. Click any line in the graph to view information at that interval. The X-axis represents time and the Y-axis represents the number of bytes. The X-axis will be in seconds, minutes, hours, days, or months depending on which tab was selected. The color of the bar will normally appear in blue, but if an alarm threshold was set and exceeded then the bar will be in red.
4. Click **Update Now** to refresh the screen based on the most recent data available.
5. Click **Download to File** in the lower left-hand corner of the screen to save the data for review and analysis. The data can be saved to your local C: drive in a *.txt format. The file contents are tab-delimited.

Alarms

To set alarms for a policy, you must enable counters and set alarm thresholds for that policy. See "Define a policy" on page 3-19 for more information.

You can also configure the S9500 to alert you via e-mail whenever an alarm is triggered. For more information, see "E-mail Alert Notification" on page 3-30.

To view and save information on an alarm:

1. From the Web browser, in the Web Administration Tools, click the **Monitor: Alarm** button. The Alarm page, with Traffic Alarm and Event Alarm tabs, appears. Select either tab to view those alarms.
2. Click **Recent Alarm Time** to view information about specific alarms. The Alarm Details page appears.
3. Click **Download to File** in the lower left-hand corner of the screen to save the data for review and analysis. The data can be saved to your local C: drive in a *.txt format. The file contents are tab-delimited.

4. Click **Clear Alarms** to erase all the data.
5. Click **Next** or **Previous** to move to the corresponding page.

Logs

Two types of logs are maintained: one for system events and one for traffic policies. To have the S9500 keep logs, you must enable logs for that policy. See “Define a policy” on page 3-19 for more information.

To view and save information on a log:

1. From the Web browser, in the Web Administration Tools, click the **Monitor: Log** button. The Log Table page, with Traffic Log and Event Log tabs, appears. Select either tab to view that log.
2. In the Action column, click **View Log Entries** for that policy’s log. The Log Details page appears.
3. Click **Download to File** in the lower left-hand corner of the screen to save the data for review and analysis. The data can be saved to your local C: drive in a *.txt format. The file contents are tab-delimited.
4. Click **Clear Log** to clear the log after downloading the most recent data available.

Chapter 4

Configuration Examples

This chapter provides examples of four ways you can configure the S9500. Each example consists of step-by-step instructions on how to configure the unit as well as guidelines on how the hosts should be configured.

These examples assume you have already configured the S9500 for Transparent mode, as shown in the Getting Started Guide included in your Netopia folio.

The four examples presented here are:

- “Example 1: Transparent Mode” on page 4-45

  Best for simple firewall protection; this configuration expands on the Quick Configuration explained in the Getting Started Guide included in your Netopia folio.

- “Example 3: 3-port Network Address Translation mode” on page 4-58

  Best for new Internet connections where the site will host public servers (web, e-mail) that require different security policies. All 3 ports are used.

- “Example 2: 2-port Network Address Translation Mode” on page 4-52

  Best for new Internet connections where the ISP provides fewer IP addresses than existing or planned devices. Only 2 ports (Trusted, Untrusted) are used; the DMZ port is not used.

- “Example 4: Virtual Private Network (VPN) Tunnel” on page 4-64

  Best for established Internet connections seeking to access the S9500 remotely.

Examples 2, 3, and 4 use the Network Address Translation mode, which is explained in “Network Address Translation mode” on page 3-24.

Note: When using NAT, the IP address set for the Trusted Interface/Inside IP Trusted Interface will be used as the default gateway for all hosts that need Internet access.

Therefore, unless a separate router/gateway system is set up inside your internal network, all hosts must be located on the same subnet as the Trusted network in order to gain Internet access. Also, the DNS (Domain Name Server) must be defined on each host and should be supplied by the ISP if not run locally. No DNS entry is required for the S9500.

Example 1: Transparent Mode

This configuration expands on the basics of the Transparent mode, as described in the Getting Started Guide included in your Netopia folio. Transparent mode uses 2 ports, the Trusted and Untrusted ports; the DMZ port is not used.

This configuration allows internal users to access the Internet and receive email and allows remote sites to access the FTP Server. This configuration would be useful for a simple network requiring firewall protection.

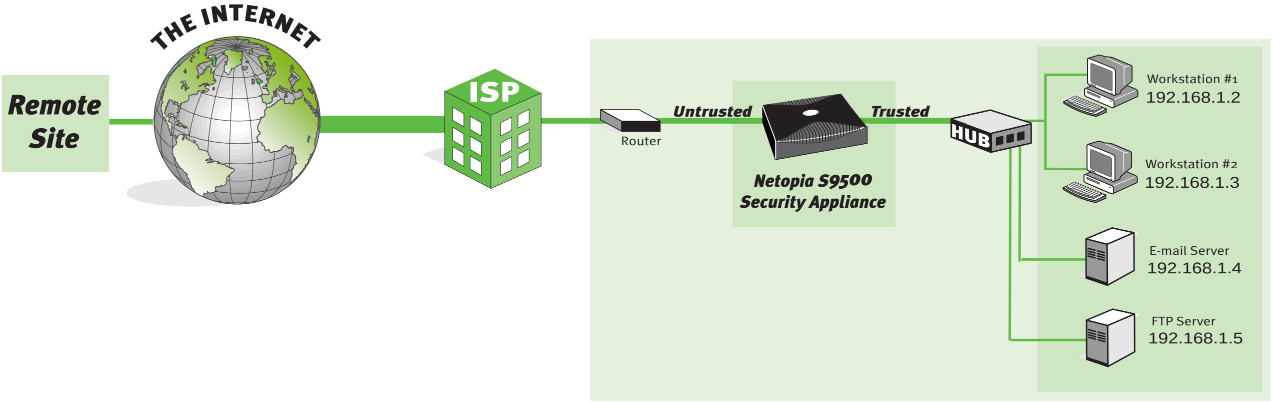
The goals of this example are to:

- Permit outgoing Internet access for Workstation (WS) #1 and WS #2
- Permit the internal Mail Server to receive and send mail to the Internet
- Permit a remote site to access the FTP Server
- Use WS #1 as the administration workstation

This example assumes:

- The S9500 has been installed into the network.
- The S9500 was configured in Transparent mode.

Your network should resemble this diagram:



Verify Configuration of the S9500

To begin this example, first log on to the S9500 Web management page, and verify that the S9500 is in Transparent mode by checking the interface settings.

1. From the Web browser, in the Web Administration Tool menu, click the **System: Configure** button and select the Interface tab. The Interface page appears.
2. Only the **Web Management Interface** field should have an IP value. In Transparent mode, all other interface IP address are 0.0.0.0.

Set Up Addresses

The next step of this example is to define the workstations and servers that need to pass through the firewall.

1. To define these machines, set up their addresses. In the menu, click on the **Lists: Address** button. The Address Book with Trusted and Untrusted tabs appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labelled “Trusted”. These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labelled “Untrusted”. These entries appear in red on your screen.

2. Click **New Address** in the lower left-hand corner of the screen. The Address Configuration page appears.

3. Enter the following information:

Field	Information
Address Name:	WS #1 (A descriptive name that must be unique from other address book entries)
IP Address:	192.168.1.2
NetMask:	255.255.255.255
Comment:	(e.g., Administration workstation)
Location:	Trusted

4. Click **OK** and the Address Book page reappears.

   Note: If you made a mistake, click **Edit**.

5. Repeat the process for WS #2. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	WS #2 (A descriptive name that must be unique from other address book entries)
IP Address:	192.168.1.3
NetMask:	255.255.255.255
Comment:	(e.g., WS #2)
Location:	Trusted

6. Click **OK** and the Address Book page reappears.

7. Repeat the process for the Mail Server. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	Mail Server (A descriptive name that must be unique from other address book entries)
IP Address:	192.168.1.4

Field	Information
NetMask:	255.255.255.255
Comment:	(e.g., Mail Server)
Location:	Trusted

8. Click **OK** and the Address Book page reappears.
9. Repeat the process for the FTP Server. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	FTP Server (A descriptive name that must be unique from other address book entries)
IP Address:	192.168.1.5
NetMask:	255.255.255.255
Comment:	(e.g., FTP Server)
Location:	Trusted

10. Click **OK** and the Address Book page reappears. It now shows the 5 defined Trusted ports.
11. Repeat the process for the remote site. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	Remote Site (A descriptive name that must be unique from other address book entries)
IP Address:	209.45.8.201
NetMask:	255.255.255.255
Comment:	(e.g., Remote Site)
Location:	Untrusted

12. Click **OK** and the Untrusted Address Book page appears. It now shows the 1 defined Untrusted port.

Set Up the Outgoing Policy

Next you must set up a policy to permit outside access to the Web site. In this example, you need to define policies to:

- Permit Internet access from WS #1 and WS #2
- Permit mail from and to the Internet

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Remove the policy permitting any inside traffic to any outside address that you created in the initial configuration. In the Configure column, click **Remove** and a confirmation message will appear. Select **Yes**.
3. To add a new policy, in the Access Policies page, select the Outgoing tab and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.
4. Define a policy that permits Internet access from WS #1. Enter the following information:

Field	Information
Source Address:	WS #1 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

Note: A policy can be more selective by selecting individual services.

5. Repeat the process for WS #2. Enter the following information:

Field	Information
Source Address:	WS #2 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

6. Repeat the process for outgoing e-mail from the Mail Server. Enter the following information:

Field	Information
Source Address:	Mail Server (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	Mail (available in the pop-up window)
Action:	Permit (available in the pop-up window)

   Leave the rest of the options at their default values. Click the **OK** button.

7. Repeat the process for outgoing DNS from the Mail Server. Enter the following information:

Field	Information
Source Address:	Mail Server (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	DNS (available in the pop-up window)
Action:	Permit (available in the pop-up window)

   Leave the rest of the options at their default values. Click **OK**. The Access Policies page appears. The Outgoing tab now displays the four new policies.

Test the Configuration

To confirm the outgoing policies work, from WS #1, use a Web browser to access an external Web site (e.g., www.netopia.com). You should be able to locate the site and access the available Web pages.

Set up the Incoming Policy

Now define a Policy that permits incoming access, in this example, for the Mail Server and the FTP Server.

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Incoming tab, and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.

3. To define a policy that permits mail to the Mail Server, enter the following information:

Field	Information
Source Address:	Outside Any (available in the pop-up window)
Destination Address:	Mail Server (available in the pop-up window)
Service:	Mail (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

4. Repeat the process to allow the Remote Site access to the FTP Server. Enter the following information:

Field	Information
Source Address:	Remote Site (available in the pop-up window)
Destination Address:	FTP Server (available in the pop-up window)
Service:	FTP (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**. The Access Policies page appears. The Incoming tab now displays the two new policies.

Test the Configuration

To confirm the incoming policies work, from the remote site, try to access the FTP server. The remote site should be able to connect. Then, from WS #1, use an e-mail service to send e-mail to your site.

You have completed this example of expanding the basic configuration of the Transparent mode. For more information on configuration, see the *Netopia S9500 Security Appliance Reference Guide* included on your Netopia CD.

You have completed Example 1.

Example 2: 2-port Network Address Translation Mode

This configuration is best for new Internet connections where the ISP provides fewer IP addresses than existing or planned devices require. Only 2 ports are used, the Trusted and Untrusted ports; the DMZ port is not used.

This configuration enables Network Address Translation (NAT) and allows users to access the Internet. This configuration would be required if you were adding a new Internet connection and did not plan to have public servers or were replacing a 2-port security solution and did not want to reconfigure the network.

Note: For security reasons, if you need to have public servers (e.g., Web or mail), you should place them on the DMZ port with their own security policy. See “Example 3: 3-port Network Address Translation mode” on page 4-58.

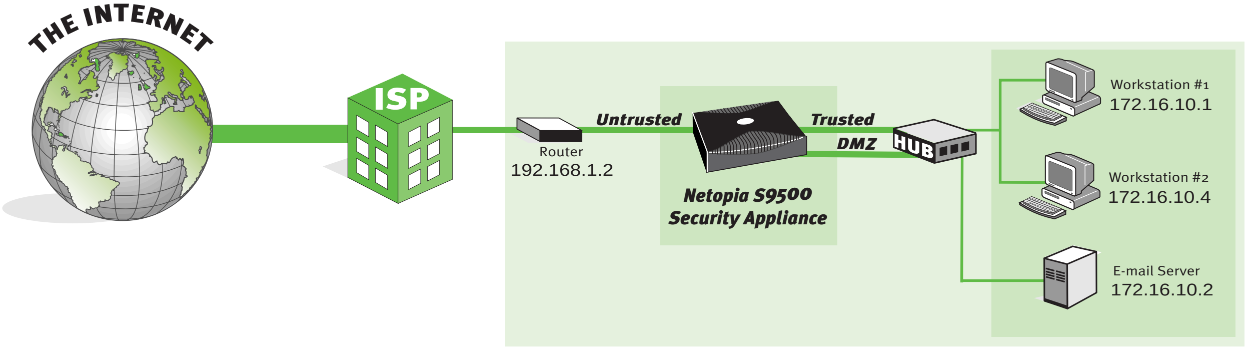
The goals of this example are to:

- Permit outgoing Internet access for Workstation (WS) #1 and WS #2
- Permit the internal mail server to be accessed through its Virtual IP address.
- Use WS #1 as the administration workstation

This example assumes:

- The S9500 has been installed into the network.
- The S9500 was configured in Transparent mode.

Your network should resemble this diagram:



To begin this example, first gather all the information you will need to configure Network Address Translation (NAT). Determine what address range will be used for the Untrusted and Trusted addresses. This example uses the following information:

- Internet Router IP: 192.168.1.2 (assigned by the ISP, connected to the Untrusted port)
- Internet Router subnet mask 255.255.255.0 (assigned by the ISP)
- S9500 Untrusted IP: 192.168.1.1 (must be on the same subnet as the Internet router)
- S9500 Untrusted subnet mask: 255.255.255.0 (must be on the same subnet as the Internet router)
- S9500 Trusted IP: 172.16.10.3 (all hosts must be on the same subnet)
- S9500 Trusted subnet mask: 255.255.255.0 (all hosts must be on the same subnet)

- External Mail Server legal Internet address 192.168.1.3 (must be on the same subnet as the Internet router)
- Internal Mail Server NAT address 172.16.10.2 (must be on the same subnet as the internal network)

Then log on to the S9500 Web management page.

Configure the S9500 for NAT

1. From the Web browser, in the Web Administration Tool menu, click the **System: Configure** button and select the Interface tab. The Interface page appears.
2. Enter the following information:

Field	Information
Web Management Interface, System IP	0.0.0.0
Web Management Interface, Port	80
Trusted Interface, Inside IP	172.16.10.3 This IP will now be used to access the management IP.
Trusted Interface, NetMask	255.255.255.0
Trusted Interface, Default Gateway	0.0.0.0
Untrusted Interface, Outside IP	192.168.1.1
Untrusted Interface, NetMask	255.255.255.0
Untrusted Interface, Default Gateway	192.168.1.2
DMZ Interface	0.0.0.0

Note: The 2-port NAT mode is automatically enabled if you enter a routable address on the Untrusted IP address and a private IP address on the Trusted IP address.

3. Click **Save and Reset**. In the confirmation screen, click **Yes**.
4. In the system warning message box, click **OK**.
5. Exit the Web browser, without clicking **Yes**.
6. Reconfigure the administration workstation so it is on the same subnet as the Trusted interface of the S9500. You may have to restart the workstation.

The Trusted interface IP is 172.16.10.3 and the subnet mask is 255.255.255.0, so the administration workstation IP must be in the range from 172.16.10.1 to 172.16.10.253.

This example uses WS #1 as the administration workstation, so change its IP address to 172.16.10.1.

Note: You will have to reconfigure all other workstations to be in same IP range and redefine all workstations to have the same default gateway as the S9500's Trusted IP. For more information, see the discussion of NAT in "Network Address Translation mode" on page 3-24.

7. Change WS #2's IP address to 172.16.10.4.
8. Change the Mail Server's IP address to 172.16.10.2.

Test the Configuration

To confirm the configuration is correct, use the Web browser to access an external web site (e.g., www.netopia.com). You should be able to locate the site and access the available web pages.

Set Up Addresses

The next step of this example is to define the workstations and servers that need to pass through the firewall.

1. Log on to the S9500 Web management page by entering the new Trusted interface IP address, http://172.16.10.3/ into the Web browser.
2. In the Web Administration Tools menu, click the **Lists: Address** button. The Address Book page, with Trusted and Untrusted tabs, appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labelled "Trusted". These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labelled "Untrusted". These entries appear in red on your screen.
3. Click **New Address** in the lower left-hand corner of the screen. The Address Configuration page appears.
4. Enter the following information:

Field	Information
Address Name:	WS #1 (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.10.1
NetMask:	255.255.255.255
Comment:	(e.g., Administration workstation)
Location:	Trusted

5. Click **OK** and the Address Book page reappears.

   Note: If you made a mistake, click **Edit**.

6. Repeat the process for WS #2. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	WS #2 (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.10.4
NetMask:	255.255.255.255
Comment:	(e.g., WS #2)
Location:	Trusted

7. Click **OK** and the Address Book page reappears.
8. Repeat the process for the Mail Server. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	Mail Server (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.10.2
NetMask:	255.255.255.255
Comment:	(e.g., Mail Server)
Location:	Trusted

9. Click **OK**.

Set Up Policy

Next you must set up a policy to permit outside access to the Web site. In this example, you need to define policies to:

- Permit Internet access from WS #1 and WS #2
- Permit mail from and to the Internet

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Remove the old policy permitting any inside to outside traffic. In the Configure column, click **Remove** and a confirmation message will appear. Select **Yes**.
3. To add a new policy, in the Access Policies page, select the Outgoing tab and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.
4. Define a policy that permits Internet access from WS #1. Enter the following information:

Field	Information
Source Address:	WS #1 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

   Leave the rest of the options at their default values. Click **OK**.

   Note: A policy can be more selective by selecting individual services.

5. Repeat the process for WS #2. Enter the following information:

Field	Information
Source Address:	WS #2 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

   Leave the rest of the options at their default values. Click **OK**.

Configure Virtual IP

The next step is to allow Internet traffic to reach the internal mail server by defining a Virtual IP address on the Untrusted side of the S9500. Virtual IP allows a hole to be opened in the firewall allowing traffic to pass to the internal network. Extreme caution should be taken when defining a Virtual IP.

1. In the Web Administration Tools menu, click the **Network: Virtual IP** button. The Virtual IP page appears.
2. Select the Virtual IP 1 tab and click the link to configure Virtual IP. The Virtual IP Configuration page appears.
3. Define the **Virtual IP Address** by entering 192.168.1.3.
4. Click **OK**, and the Virtual IP page reappears.
5. Select **New Services** in the lower left-hand corner of the screen. The Virtual IP Service Configuration page appears.
6. To define the Virtual IP Service for mail, enter the following information:

Field	Information
Virtual Port:	25 (for mail)
Service:	Mail (available in the pop-up window)
Server IP #1:	172.16.10.2

Click **OK**.

7. The defined service now appears in the table on the Virtual IP page.

Now define a policy that permits only incoming mail server access.

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Incoming tab, and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears
3. Enter the following information:

Field	Information
Source Address:	Outside Any (available in the pop-up window)
Destination Address:	VIP 192.168.1.3 (available in the pop-up window)

Field	Information
Service:	Mail (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

You have completed Example 2.

Example 3: 3-port Network Address Translation mode

This configuration is best for new Internet connections that will host public servers (e.g., Web, e-mail), requiring a different security policy. The third port, DMZ, will be used.

This configuration enables NAT and allows all users to have access to the Internet and allows outside access to the DMZ hosts only. This configuration would be required if you were adding an Internet connection and security solution.

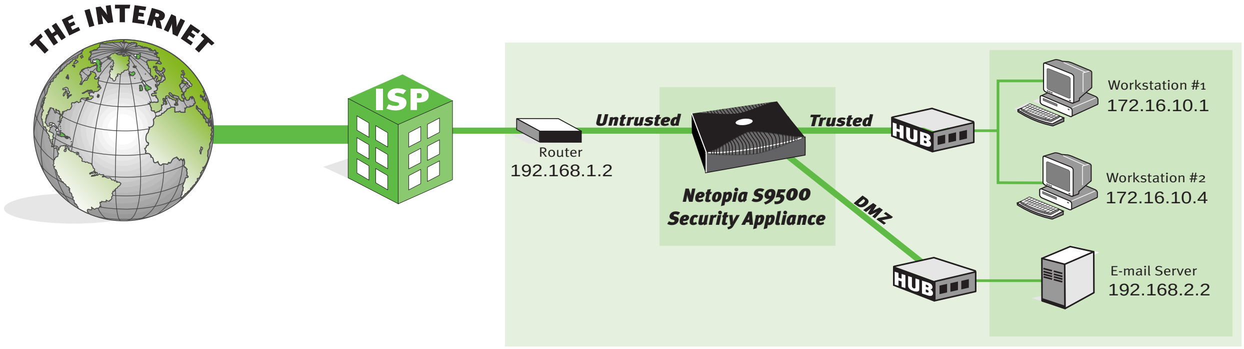
The goals of this example are to:

- Permit outgoing Internet access for Workstation (WS) #1 and WS #2
- Permit the DMZ mail server to be accessed from the Internet by assigning it a routable IP address.
- Use WS #1 as the administration workstation

This example assumes:

- The S9500 has been installed into the network.
- The S9500 was configured in Transparent mode.

Your network should resemble this diagram:



To begin this example, first gather all the information you will need to configure Network Address Translation (NAT). Determine what address range will be used for the Untrusted and Trusted addresses. This example uses the following information:

- Internet Router IP: 192.168.1.2 (assigned by the ISP, connected to the Untrusted port)
- Internet Router subnet mask 255.255.255.0 (assigned by the ISP)
- S9500 Untrusted IP: 192.168.1.1 (must be on the same subnet as the Internet router)
- S9500 Untrusted subnet mask: 255.255.255.0 (must be on the same subnet as the Internet router)
- S9500 Trusted IP: 172.16.10.3 (all hosts must be on the same subnet)
- S9500 Trusted subnet mask: 255.255.255.0 (all hosts must be on the same subnet)
- S9500 DMZ IP: 192.168.2.1 (must be on a separate subnet from the Untrusted hosts)
- S9500 DMZ subnet mask: 255.255.255.0 (all DMZ hosts must be on the same subnet)
- Mail Server legal Internet address 192.168.2.2 (must be on the same subnet as the Internet router)

Then log on to the S9500 Web management page.

Configure the S9500 for NAT

1. From the Web browser, in the Web Administration Tool menu, click the **System: Configure** button and select the Interface tab. The Interface page appears.
2. Enter the following information:

Field	Information
Web Management Interface, System IP	0.0.0.0
Web Management Interface, Port	80
Trusted Interface, Inside IP	172.16.10.3 This IP will now be used to access the management IP.
Trusted Interface, NetMask	255.255.255.0
Trusted Interface, Default Gateway	0.0.0.0
Untrusted Interface, Outside IP	192.168.1.1
Untrusted Interface, NetMask	255.255.255.0
Untrusted Interface, Default Gateway	192.168.1.2 (Internet Router IP address)

Field	Information
DMZ Interface	192.168.2.1
DMZ NetMask	255.255.255.0

3. Click **Save and Reset**. In the confirmation screen, click **Yes**.
4. In the system warning message box, click **OK**.
5. Exit the Web browser, without clicking **Yes**.
6. Reconfigure the administration workstation so it is on the same subnet as the Trusted interface of the S9500. You may have to restart the workstation.

   The Trusted interface IP is 172.16.10.3 and the subnet mask is 255.255.255.0, so the administration workstation IP must be in the range from 172.16.10.1 to 172.16.10.253.

   This example uses WS #1 as the administration workstation, so change its IP address to 172.16.10.1.

   Note: You will have to reconfigure all other workstations to be in same IP range and redefine all workstations to have the same default gateway as the S9500's Trusted IP. For more information, see the discussion of NAT in "Network Address Translation mode" on page 3-24. Workstations on the DMZ port will have to use the DMZ.
7. Change WS #2's IP address to 172.16.10.4.
8. Change the Mail Server's IP address to 192.168.2.2.

Test the Configuration

To confirm the configuration is correct, use the Web browser to access an external web site (e.g., www.netopia.com). You should be able to locate the site and access the available web pages.

Set Up Address

The next step of this example is to define the workstations and servers that need to pass through the firewall.

1. Log on to the S9500 Web management page by entering the new Trusted interface IP address, http://172.16.10.3/ into the Web browser.
2. In the Web Administration Tools menu, click the **Lists: Address** button. The Address Book page, with Trusted and Untrusted tabs, appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labelled "Trusted". These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labelled "Untrusted". These entries appear in red on your screen.
3. Click **New Address** in the lower left-hand corner of the screen. The Address Configuration page appears.

4. Enter the following information:

Field	Information
Address Name:	WS #1 (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.10.1
NetMask:	255.255.255.255
Comment:	(e.g., Administration workstation)
Location:	Trusted

5. Click **OK** and the Address Book page reappears.

   Note: If you made a mistake, click **Edit**.

6. Repeat the process for WS #2. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	WS #2 (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.10.4
NetMask:	255.255.255.255
Comment:	(e.g., WS #2)
Location:	Trusted

7. Click **OK** and the Address Book page reappears.

8. Repeat the process for the Mail Server. Click **New Address**. The Address Configuration page appears. Enter the following information:

Field	Information
Address Name:	Mail Server (A descriptive name that must be unique from other address book entries)

Field	Information
IP Address:	192.168.2.2
NetMask:	255.255.255.255
Comment:	(e.g., Mail Server)
Location:	DMZ

9. Click **OK**.

Set Up the Outgoing Policy

Next you must set up a policy to permit outside access to the Internet.

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Remove the old policy permitting any inside to outside traffic. In the Configure column, click **Remove** and a confirmation message will appear. Select **Yes**.
3. To add a new policy, in the Access Policies page, select the Outgoing tab and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.
4. Define a policy that permits Internet access from WS #1. Enter the following information:

Field	Information
Source Address:	WS #1 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

Note: A policy can be more selective by selecting individual services.

5. Repeat the process for WS #2. Enter the following information:

Field	Information
Source Address:	WS #2 (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

Set up the Incoming Policy

Now define policies that permit Mail and POP3 to the DMZ from the outside.

1. In the Web Administration Tools menu, click the **Network: Policy** button. Select the To DMZ tab and click **New Policy** in the lower left-hand corner of the screen.
2. To define the policy for mail, enter the following information:

Field	Information
Source Address:	Inside Any (available in the pop-up window)
Destination Address:	Mail Server (available in the pop-up window)
Service:	MAIL (available in the pop-up window)
Action:	Permit (available in the pop-up window)

Leave the rest of the options at their default values. Click **OK**.

3. Repeat the process for POP3 and for DNS.

Test the Configuration

To confirm the configuration is correct, use the Web browser at WS #1 to access an external web site (e.g., www.netopia.com). You should be able to locate the site and access the available web pages.

You have completed Example 3.

Example 4: Virtual Private Network (VPN) Tunnel

This configuration illustrates how to set up a Virtual Private Network (VPN) between two offices located in Los Angeles and Chicago. Both S9500 units are configured for Network Address Translation (NAT). The function of the S9500 is to perform encryption/decryption on each packet at either end of the tunnel. This operation ensures the security and the privacy of communication over the public network backbone such as the Internet.

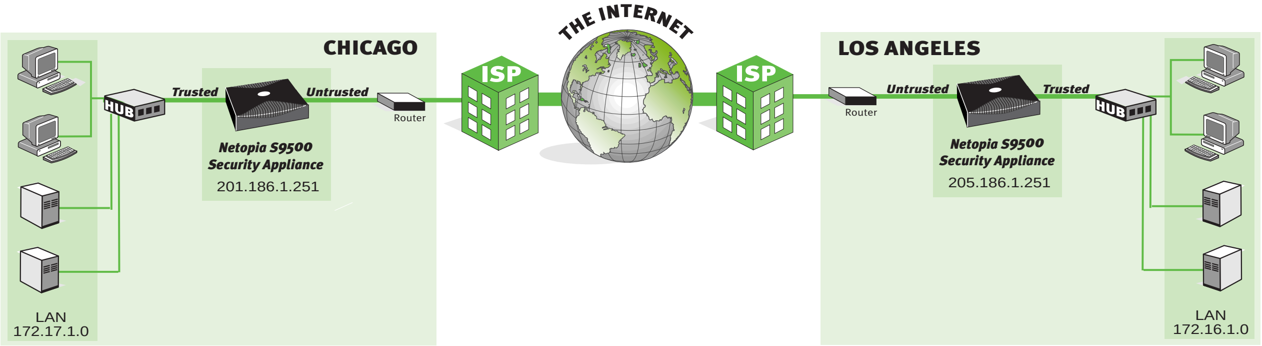
The goals of this example are to:

- Secure the VPN tunnel for all services to the Chicago office network
- Permit outgoing Internet Web access for everybody in the office network

This example assumes:

- The S9500 has been installed into the network.
- The S9500 was configured in Transparent mode.

Your network should resemble this diagram:



To begin this example, configure the Los Angeles site. First gather all the information you will need to configure Network Address Translation (NAT). Determine what address range will be used for the Untrusted and Trusted addresses. This example uses the following information:

- Internet Router IP: 205.186.1.254 (assigned by the ISP, connected to the Untrusted port)
- Internet Router subnet mask 255.255.255.0 (assigned by the ISP)
- S9500 Untrusted IP: 205.186.1.251 (must be on the same subnet as the Internet router)
- S9500 Untrusted subnet mask: 255.255.255.0 (must be on the same subnet as the Internet router)
- S9500 Trusted IP: 172.16.1.251 (all hosts must be on the same subnet)
- S9500 Trusted subnet mask: 255.255.255.0 (all hosts must be on the same subnet)
- LA network: 172.16.1.0
- LA subnet mask: 255.255.255.0

Then log on to the S9500 Web management page.

Configure the S9500 for NAT

1. From the Web browser, in the Web Administration Tool menu, click the **System: Configure** button and select the Interface tab. The Interface page appears.
2. Enter the following information:

Field	Information
Web Management Interface, System IP	0.0.0.0
Web Management Interface, Port	80
Trusted Interface, Inside IP	172.16.1.251 This IP will now be used to access the management IP.
Trusted Interface, NetMask	255.255.255.0
Trusted Interface, Default Gateway	0.0.0.0
Untrusted Interface, Outside IP	205.186.1.251
Untrusted Interface, NetMask	255.255.255.0
Untrusted Interface, Default Gateway	205.186.1.254
DMZ Interface	0.0.0.0

3. Click **Save and Reset**. In the confirmation screen, click **Yes**.
4. In the system warning message box, click **OK**.
5. Reconfigure the administration workstation so it is on the same subnet as the Trusted interface of the S9500. You may have to restart the workstation.

   The Trusted interface IP is 172.16.1.251 and the subnet mask is 255.255.255.0, so the administration workstation IP must be in the range from 172.16.1.1 to 172.16.1.253.

   This example uses WS #1 as the administration workstation, so change its IP address to 172.16.1.1.

   Note: You will have to reconfigure all other workstations to be in same IP range and redefine all workstations to have the same default gateway as the S9500's Trusted IP. For more information, see the discussion of NAT in "Network Address Translation mode" on page 3-24.

Set Up Addresses

The next step of this example is to define the workstations and servers that need to pass through the firewall.

1. Log on to the S9500 Web management page by entering the new Trusted interface IP address, http://172.16.1.251/ into the Web browser.
2. In the Web Administration Tools menu, click the **Lists: Address** button. The Address Book page, with Trusted and Untrusted tabs, appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labelled "Trusted". These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labelled "Untrusted". These entries appear in red on your screen.
3. Click **New Address** in the lower left-hand corner of the screen. The Address Configuration page appears.
4. Enter the following information:

Field	Information
Address Name:	LA_LAN (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.1.0
NetMask:	255.255.255.0
Comment:	(e.g., Los Angeles office network)
Location:	Trusted

   Click **OK** to save the entry.
5. Repeat the procedure to add the Chicago office network address to the Untrusted side. In the Address Configuration page, enter the following information:

Field	Information
Address Name:	CHI_LAN (A descriptive name that must be unique from other address book entries)
IP Address:	172.17.1.0
NetMask:	255.255.255.0
Comment:	(e.g., Chicago office network)
Location:	Untrusted

   Click **OK** to save the entry.

Set Up VPN

Next, configure the S9500 for VPN.

1. In the Web Administration Tools menu, click the **Network: VPN** button. The VPN Lists page appears. Select the Manual Key tab.
2. Click **New VPN Entry** in the lower left-hand corner of the screen. The Manual Key VPN Configuration page appears.
3. Enter the following information:

Field	Information
VPN Name:	LA-CHI
Gateway IP:	201.186.1.251 (This is the Untrusted IP address of the S9500 in Chicago.)
Security Index (Local):	16100
Security Index (Remote):	17100
ESP-DES Algorithm:	3DES-CBC
HEX Key:	c2c4c70101010101 f8899b6e6d7c8f9e 4f5b68b094a4b6c7
Generated Key by Password:	(don’t use)
ESP-Authentication Algorithm:	MD5
HEX Key:	c8cbcd0101010101 and a4b6439e8c9faeb12
Generated Key by Password:	(don’t use)

Click **OK** to save the entry.

Set Up Policy

To support VPN, the S9500 also must support encryption. So now you must set up an encryption policy, and then a policy to permit Web access.

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Outgoing tab and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.

3. Define a policy for encryption. Enter the following information:

Field	Information
Source Address:	LA_LAN (available in the pop-up window)
Destination Address:	CHI_LAN (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Encrypt (available in the pop-up window)
VPN Tunnel:	LA_CHI (available in the pop-up window)

Click **OK**.

Note: A policy can be more selective by selecting individual services.

4. Define a policy for Internet Web access. Enter the following information:

Field	Information
Source Address:	Inside Any (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	HTTP (available in the pop-up window)
Action:	Permit (available in the pop-up window)
VPN Tunnel:	LA_CHI (available in the pop-up window)

Click **OK**.

Configure the Second Site

Now configure the Chicago site.

Gather all the information needed to configure NAT. Determine what address range will be used for the Untrusted and Trusted addresses. This example uses the following IP address:

- Internet Router IP: 201.186.1.254
- Internet Router subnet mask: 255.255.255.0
- S9500 Untrusted IP: 201.186.1.251
- S9500 Untrusted subnet mask: 255.255.255.0
- S9500 Trusted IP: 172.17.1.251
- S9500 Trusted subnet mask: 255.255.255.0
- CHI network: 172.17.1.0
- CHI subnet mask: 255.255.255.0

Then log on to the S9500 Web management page.

Configure the S9500 for NAT

1. From the Web browser, in the Web Administration Tool menu, click the **System: Configure** button and select the Interface tab. The Interface page appears.
2. Enter the following information:

Field	Information
Web Management Interface, System IP	0.0.0.0
Web Management Interface, Port	80
Trusted Interface, Inside IP	172.17.1.251 This IP will now be used to access the management IP.
Trusted Interface, NetMask	255.255.255.0
Trusted Interface, Default Gateway	0.0.0.0
Untrusted Interface, Outside IP	201.186.1.251
Untrusted Interface, NetMask	255.255.255.0
Untrusted Interface, Default Gateway	201.186.1.254
DMZ Interface	0.0.0.0

3. Click **Save and Reset**. In the confirmation screen, click **Yes**.
4. In the system warning message box, click **OK**.
5. Reconfigure the administration workstation so it is on the same subnet as the Trusted interface of the S9500. You may have to restart the workstation.

   The Trusted interface IP is 172.17.1.251 and the subnet mask is 255.255.255.0, so the administration workstation IP must be in the range from 172.17.1.1 to 172.17.1.253.

   This example uses WS #1 as the administration workstation, so change its IP address to 172.17.1.1.

   Note: You will have to reconfigure all other workstations to be in same IP range and redefine all workstations to have the same default gateway as the S9500's Trusted IP. For more information, see the discussion of NAT in "Network Address Translation mode" on page 3-24.

Set Up Addresses

The next step of this example is to define the workstations and servers that need to pass through the firewall.

1. Log on to the S9500 Web management page by entering the new Trusted interface IP address, http://172.17.1.251/ into the Web browser.
2. In the Web Administration Tools menu, click the **Lists: Address** button. The Address Book page, with Trusted and Untrusted tabs, appears.

   Trusted addresses are individual IP addresses or subnets located behind the port labelled "Trusted". These entries appear in green on your screen. Untrusted addresses are individual IP addresses or subnets located behind the port labelled "Untrusted". These entries appear in red on your screen.
3. Click **New Address** in the lower left-hand corner of the screen. The Address Configuration page appears.
4. Enter the following information:

Field	Information
Address Name:	CHI_LAN (A descriptive name that must be unique from other address book entries)
IP Address:	172.17.1.0
NetMask:	255.255.255.0
Comment:	(e.g., Chicago office network)
Location:	Trusted

   Click **OK** to save the entry.

5. Repeat the procedure to add the Los Angeles office network address to the Untrusted side. In the Address Configuration page, enter the following information:

Field	Information
Address Name:	LA_LAN (A descriptive name that must be unique from other address book entries)
IP Address:	172.16.1.0
NetMask:	255.255.255.0
Comment:	(e.g., Los Angeles office network)
Location:	Untrusted

Click **OK** to save the entry.

Set Up VPN

Next, configure the S9500 for VPN.

1. In the Web Administration Tools menu, click the **Network: VPN** button. The VPN Lists page appears. Select the Manual Key tab.
2. Click **New VPN Entry** in the lower left-hand corner of the screen. The Manual Key VPN Configuration page appears.
3. Enter the following information:

Field	Information
VPN Name:	CHI-LA
Gateway IP:	205.186.1.251 (This is the Untrusted IP address of the S9500 in Los Angeles.)
Security Index (Local):	17100
Security Index (Remote):	16100
ESP-DES Algorithm:	3DES-CBC
HEX Key:	c2c4c70101010101 f8899b6e6d7c8f9e 4f5b68b094a4b6c7
Generated Key by Password:	(don't use)

ESP-Authentication Algorithm:	MD5
HEX Key:	c8cbcd0101010101 and a4b6439e8c9faeb12
Generated Key by Password:	(don't use)

Click **OK** to save the entry.

Set Up Policy

To support VPN, the S9500 also must support encryption. So now you must set up an encryption policy, and then a policy to permit Web access.

1. In the Web Administration Tools menu, click the **Network: Policy** button. The Access Policies page appears.
2. Select the Outgoing tab and click **New Policy** in the lower left-hand corner of the screen. The Policy Configuration page appears.
3. Define a policy for encryption. Enter the following information:

Field	Information
Source Address:	CHI_LAN (available in the pop-up window)
Destination Address:	LA_LAN (available in the pop-up window)
Service:	ANY (available in the pop-up window)
Action:	Encrypt (available in the pop-up window)
VPN Tunnel:	CHI_LA (available in the pop-up window)

Click **OK**.

Note: A policy can be more selective by selecting individual services.

4. Define a policy for Internet Web access. Enter the following information:

Field	Information
Source Address:	Inside Any (available in the pop-up window)
Destination Address:	Outside Any (available in the pop-up window)
Service:	HTTP (available in the pop-up window)
Action:	Permit (available in the pop-up window)
VPN Tunnel:	CHI_LA (available in the pop-up window)

Click **OK**.

Now, a tunnel is set up between the Los Angeles and Chicago offices.

Secure Remote Administration via VPN Tunnel

After you have set up a VPN tunnel, you can securely administrate a remote S9500 through that VPN tunnel. For this example, you can add a remote administration station at Chicago to access the S9500 in Los Angeles.

1. In the Web Administration Tools menu, click the **System: Admin** button. The Administration page appears, with the Admin. and Sys Log tabs. Select the Admin. tab.
2. To restart administration from the remote address, enter the IP address and subnet mask of the client doing the remote administration:

Field	Information
Management Client IP:	172.17.1.10
Netmask:	255.255.255.255
Enable Untrusted Side Logon:	select to enable

3. Click **Apply**.

You have completed Example 4.

Chapter 5

Troubleshooting

This chapter is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia S9500. It also includes information on how to contact Netopia Technical Support.

This chapter covers the following topics:

The S9500 does not power on

When you power on the S9500, verify it has started successfully by confirming the green power supply LED lights and the status light is blinking.

The S9500 takes about 30 seconds to boot. Please wait until the status LED is blinking.

Cannot connect to the Internet

If you are not able to access the Internet, double-check:

- The Link lights on S9500, hosts, hubs and router are lit.
- The Host IP and subnet mask are configured correctly for your configuration.
- The Host gateway is defined in the host and points to the correct destination (i.e., the router if in Transparent mode, the Trusted Interface if in Network Address Translation mode).
- The Host has a valid DNS entry.
- DNS service is available through the firewall.

Link LED is off

The link LED indicates the connection status between the S9500 and the network hub. If the link LED is off, there is a problem with the network connection. Verify the Ethernet cable is properly connected and the network hub is operational. Try plugging the Ethernet cable into a different location on the hub or into a different hub. If the link LED still does not light, there may be a problem with the Ethernet adapter. Contact your Netopia Customer Service representative.

Cannot ping the S9500

If you cannot ping the S9500 from the Trusted side, your network interface is not configured properly. See your computer documentation.

If you cannot ping the S9500 from the Untrusted side, you may not have an Untrusted configuration enabled. The S9500 will not respond to ping request unless an Untrusted configuration is enabled.

Cannot ping unsecure hosts from secure hosts (or vice versa)

Each router adjacent to the firewall must contain a static route specifying the firewall as the gateway for destination networks beyond the firewall. Contact the router's administrator to verify this configuration.

Also, if your secure network uses addresses that are not registered and routable on the unsecure network, including private addresses as specified in RFC 1597, packets will not be routed back to the sender. In this case, use a client with a registered address. The firewall's Network Address Translation (NAT) feature may be used for TCP and UDP traffic, but NAT will not translate addresses in ICMP packets like ping.

Technical Support

Netopia, Inc., is committed to providing its customers with reliable products and documentation, backed by excellent technical support on-line and through our resellers and distributors.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting chapter or in other sections.

How to get support

If you contact your local reseller or distributor by telephone, please be ready to supply them with the information you used to configure the Netopia S9500 Security Appliance. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

You may also contact Netopia Technical Support directly by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)

info@netopia.com (for general information)

Phone: 1 800-782-6449

Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com

Internet via anonymous FTP to ftp.netopia.com/pub

FAX-Back

This service provides technical notes which answer the most commonly asked questions, and offer solutions for many common problems encountered with Netopia products.

FAX-Back: +1 510-814-5040

Appendix A

SNMP Support

You can use SNMP management software to administrate the Netopia S9500 Security Appliance.

The S9500's SNMP agent currently supports all MIB-II groups except EGP (Exterior Gateway Protocol) and can be monitored by any SNMP-compatible manager. The S9500 agent will generate two traps, cold start and authentication failure. The cold start trap is generated once the S9500 becomes operational following power on. The authentication failure trap is triggered if the SNMP manager sends the incorrect community string.

To configure the S9500 to communicate with the SNMP manager:

1. The SNMP manager must be on the Trusted interface side. SNMP requests from the Untrusted or DMZ port will not be processed.
2. From the Web browser, set the Administration IP address needs to the IP address of the SNMP manager.

   See the Getting Started Guide included in your Netopia folio for information on changing the Administration IP.
3. Configure the System IP and Trusted interface if you haven't already.

   See the Getting Started Guide included in your Netopia folio for information on initial configuration.
4. Reset the S9500 so the agent can initialize its SNMP manager list. The SNMP manager should now be able to communicate with the S9500's administration workstation.

Note: Ethernet Interface information is reported as 1, Trusted; 2, Untrusted; and 3, DMZ.

Note: The current implementation allows for only one SNMP manager (the administration workstation) to be defined. Requests from any other IP address will be rejected, but no trap will be generated. The community string of "public" is the default and cannot be changed.

Note: The MIB II system group variables sysContact, sysName, sysLocation, and sysServices are read/write objects. All other variables are read-only.

Appendix B

Command Line Interface

The Netopia S9500 Security Appliance can be managed via the console with typed commands. The Command Line Interface (CLI) communication requires 9600 bit rate, 8 bits, no parity, 1 stop bit, and no flow control.

Common features of the CLI

- Backspace, Delete, and Control-H can be used to remove one character.
- Control-U can be used to remove an entire line.
- Control-F and Control-B allows traversing command history buffer (up to 16 lines) forward and backward.
- Typing a question mark (?) any time during the command provides the next available keywords/input and a brief description of their usage.
- A parameter inside [] is an option, and a parameter inside {} is required.
- <a.b.c.d> is an IP address.
- <A.B.C.D> is a subnet mask.
- The console times out in 10 minutes if no keyword activity is detected.

Commands

The CLI has four basic commands: Set, Unset, Get, and Miscellaneous.

Set and Unset Commands

Set commands are used to define system parameters and are saved in non-volatile memory.

All set commands have Unset counterparts that are used to remove the configured parameters or restore to default parameters.

address

<table>
<tr><th>Syntax:</th><th>set address {trust | untrust | dmz} <string> <a.b.c.d> <A.B.C.D> [<string>]
unset address {trust | untrust | dmz} <string></th></tr>
<tr><td>Description:</td><td>set address is used to define address book entry. The first string is the name of the entry. The second string is the comment which is optional.</td></tr>
<tr><td>Default:</td><td>There are 4 system-defined address book entries:
■ Inside Any - any hosts connected to the Trusted interface
■ Outside Any - any hosts connected to the Untrusted interface
■ DMZ Any - any hosts connected to the DMZ interface
■ Dial-Up VPN - any dialup hosts to the Untrusted interface</td></tr>
<tr><td>Example:</td><td>To define an address book entry for a web server named “webserver” with IP address 184.2.50.9 and subnet mask 255.255.255.0 connected to the DMZ interface:
ns-> set address dmz webserver 184.2.50.9 255.255.255.0
To define an address book entry for a desktop machine named "odie" with IP address 172.16.10.1 and subnet mask 255.255.255.192 connected to the trusted interface with a comment of “Mary’s desktop”:
ns-> set address trust odie 172.16.10.1 255.255.255.192 "Mary's desktop"
To delete a address book entry for a partner site named “my-partner” which is connected to the untrusted interface:
ns-> unset address dmz my-partner</td></tr>
<tr><td>See Also:</td><td>get address</td></tr>
</table>

admin

Synopsis:	**set admin {name | password} <string>**
	set admin mng-ip <a.b.c.d> [<A.B.C.D>]
	set admin sys-ip <a.b.c.d>
	set admin port <number>
	set admin mail {alert | traffic-log}
	set admin mail {[mail-addr1 | mail-addr2] <string>}
	set admin mail {server-ip <address>}
	unset admin {mng-ip | name | port | sys-ip}
	unset admin mail {alert | mail-addr1 | mail-addr2 | server-ip | traffic-log}

Description:	Set admin is used to configure the administrative parameters for the S9500 device. The administrative user name is an alphanumeric string. The administrative interface port number can be changed to any number between 1024 and 32,000. The traffic log has a maximum size of 16 Kbytes. A copy of the log file is sent to the email addresses specified whenever it is full or every 24 hours, whichever comes first.
Default:	admin name and password are “netopia” mng-ip is 0.0.0.0 with subnet mask 0.0.0.0 sys-ip is 209.125.148.254 admin port is 80 mail alert is off with mail server-ip as 0.0.0.0 mail addresses are empty strings

Synopsis:	**set admin {name | password} <string>**
	set admin mng-ip <a.b.c.d> [<A.B.C.D>]
	set admin sys-ip <a.b.c.d>
	set admin port <number>
	set admin mail {alert | traffic-log}
	set admin mail {[mail-addr1 | mail-addr2] <string>}
	set admin mail {server-ip <address>}
	unset admin {mng-ip | name | port | sys-ip}
	unset admin mail {alert | mail-addr1 | mail-addr2 | server-ip | traffic-log}

Example:	To change the administrator user name to paul: ns-> set admin name paul To change the administrator login password to build4you: ns-> set admin password build4you To change the port number for the web administrative interface to 8000: ns-> set admin port 8000 To enable mail alert for administrative issues: ns-> set admin mail alert To enable mail traffic log for administrative issues: ns-> set admin mail traffic-log To configure john@abc.com as an email address to receive administrative alert: ns-> set admin mail mail-addr1 john@abc.com To specify 209.12.34.100 as the mail server to receive administrative email alert: ns-> set admin mail server-ip 209.12.34.100 To disable mail alert for administrative issues: ns-> unset admin mail alert
See Also:	get admin
Notes:	The email server that receives the administrative email alert has to be identified by its IP address. The S9500 doesn't perform name resolution. There is no way to unset the admin password. Please contact Netopia for information.

arp

Syntax:	**set arp <a.b.c.d> <A.B.C.D> <number>** **unset arp <a.b.c.d>**
Description:	set arp is used to create entry in the arp table. The S9500 supports a maximum of 256 entries. The last parameter indicates which interface the arp entry belongs to. Its value can be 0, 1, or 2 where 0 is the trusted interface, 1 is the untrusted interface, and 2 is the DMZ interface. Each entry will stay at the table for 960 seconds before it gets deleted.
Example:	To create an entry in the arp table for a machine with IP address 10.1.1.1 and MAC address 002090102345 connected to the trusted interface: ns-> set arp 10.1.1.1 002090102345 0 To create an entry in the arp table for a machine with IP address 209.234.1.2 and MAC address 000010293847 connected to the untrusted interface: ns-> set arp 209.234.1.2 000010293847 1 To create an entry in the arp table for a machine with IP address 192.1.9.23 and MAC address 00201034a98c connected to the DMZ interface: ns-> set arp 192.1.9.23 00201034a98c 2
See Also:	clear arp, get arp

auth

Syntax:	**set auth secret <string>** **set auth server-ip <ip-addr>** **set auth timeout <number>** **set auth type <auth-type>** **unset auth {secret | server-ip | timeout}** **unset auth type {0 | 1 | 2}**
Description:	set auth is used to configure the method and parameter used by the S9500 for the user authentication method selected. The methods available are the S9500 built-in database or external Radius server. The S9500 device configures the same secret string as the Radius server for protecting the message sent between them.
Default:	The S9500 Built-in User database is used. User idle timeout is 10 minutes.
Example:	To define the Radius shared secret to "mysecret": ns-> set auth secret mysecret To use the built-in user database of the S9500 device for user authentication: ns-> set auth type 0
See Also:	clear auth, get auth

clock

Syntax:	**set clock <mm/dd/yy hh:mm>**
Description:	Define the system time in the format of mm/dd/yy hh:mm which stands for month, day, year, hour, and minute. Specify the hour and minute in the 24 hour format
Example:	To define the system time as November 11, 2001 at 1:30PM: ns-> set clock 11/03/2001 13:30

console

Syntax:	set console {dbuf | disable}
	set console {page | timeout} <number>
	unset console {dbuf | disable | page | timeout}

Description:	set console is used to define the console parameters. When debug is enabled on the S9500, all debugging messages will be displayed to the console, which may be too overwhelming. Using the dbuf parameter, those messages will be stored at a buffer where they can be later retrieved by the get dbuf command. The buffer size is 256K. Console access can be disabled with the disable parameter. The action needs two confirmations. Once the command is submitted, the configuration is saved and the current login session exits. The number of lines displayed at one time to the console is configurable by the page parameter. After a period of idle time, the S9500 will automatically log out the administrator from console access. It is configurable by the time-out parameter. A value of 0 means the console will never timeout.
Default:	Displays 22 lines to the console. Timeout is 10 minutes
Example:	To redirect all debugging messages to the buffer: ns-> set console dbuf To disable console access: ns-> set console disable To define 20 lines per page displayed on the console: ns-> set console page 20 To define console timeout value to 40 minutes: ns-> set console timeout 40
See Also:	get console, clear dbuf, get dbuf

dialup-group

Syntax:	**set dialup-group <string> [{+ | -} <string>]** **unset dialup-group <string>**
Description:	set dialup-group is used to create a group so that a few remote users can be grouped together. A policy for a dialup-group applies to all members in the group.
Example:	To define a dialup user group called “telecommuters”: ns-> set dialup-group telecommuters To add a remote VPN user named “john-home” to the telecommuters group: ns-> set dialup-group telecommuters + john-home To delete a remote VPN user named “amy-home” from the telecommuters group: ns-> set dialup-group telecommuters - amy-home To delete the telecommuters group: ns-> unset dialup-group telecommuters
See Also:	get dialup-group

dip

Syntax:	**set dip <a.b.c.d>-<x.y.z.w>** **unset dip <number>**
Description:	set dip is used to dynamic IP range. Dynamic IP allocates an IP address for those applications such as rlogin and talk that use more than one IP address when the S9500 is running in NAT mode.
See Also:	get dip

ffilter

Syntax:	**set ffilter dst-ip <a.b.c.d> [dst-port <number>]** **set ffilter dst-ip <a.b.c.d> [ip-proto <number> [dst-port <number>]]** **set ffilter dst-ip <a.b.c.d> [ip-proto <number> [src-port <number>]]** **set ffilter dst-ip <a.b.c.d> [src-port <number> [dst-port <number>]]** **set ffilter dst-port <number>** **set ffilter ip-proto <number> [dst-port <number>]** **set ffilter ip-proto <number> [src-port <number> [dst-port <number>]]** **set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d> [dst-port <number>]]** **set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d> [ip-proto <number> [dst-port <number>]]]** **set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d> [ip-proto <number> [src-port <number> [dst-port <number>]]]]** **set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d> [src-port <number>]]** **set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d> [src-port <number> [dst-port <number>]]]** **set ffilter src-ip <a.b.c.d> [dst-port <number>]** **set ffilter src-ip <a.b.c.d> [ip-proto <number> [dst-port <number>]]** **set ffilter src-ip <a.b.c.d> [ip-proto <number> [src-port <number> [dst-port <number>]]]** **set ffilter src-ip <a.b.c.d> [src-port <number> [dst-port <number>]]** **set ffilter src-port <number> [dst-port <number>]** **unset ffilter**
Description:	set ffilter is used to create a filter for the debug flow output so that only traffic related to specific source address, destination address, source port, and destination port will be shown.
Example:	To create a filter for all traffic from a host with IP address 172.16.10.1: ns-> set ffilter src-ip 172.16.10.1 To create a filter for all SMTP traffic destined to a host with IP address 209.114.3.2: ns-> set ffilter dst-ip 209.114.3.2 dst-port 25 To erase all filter settings: ns-> unset ffilter
See Also:	get ffilter

firewall

Syntax:	**set firewall {default deny | ip-spoofing | ping-of-death | src-route | syn-attack | tear-drop }** **unset firewall**
Description:	set firewall is used to enable protection against various network attacks. unset firewall is used to disable protection against various network attacks. Options: ■ default deny: deny all traffic not specifically allowed by a network policy. Disabled this would allow all traffic that is not denied. ■ ip-spoofing: spoofing attacks occur when unauthorized agents attempt to bypass the firewall security by imitating valid client IP addresses. ■ ping-of-death: many ping implementations allow the user to specify a larger packet size if desired, which can trigger a range of adverse system reactions including crashing, freezing, and rebooting. ■ src-route: IP header information has an option to contain routing information that may specify a different route. ■ syn-attack: attacks occur when the connecting host continuously sends TCP syn requests without the corresponding ack response. ■ tear-drop: attacks occur when TCP packets overlap, rendering Windows 95 machines dead.
Default:	All enabled
Example:	To enable the default-deny firewall protection: ns-> set firewall default-deny To disable the ip-spoofing firewall protection: ns-> unset firewall ip-spoofing
See Also:	get firewall, set syn-threshold

globall

Syntax:	**set global { config-port | listen | report-port } port** **set global enable** **set global ip address** **set global send network [** **set global send { resource | summary }** **unset global**
Description:	Define S9500 Global configuration.
Example:	ns-> set global enable
See Also:	get global

hostname

Syntax:	**set hostname** **unset hostname**
Description:	set hostname is used to define the S9500’s hostname which appears on the console prompt.
Default:	ns
Example:	To change the S9500’s hostname to “acme”: ns-> set hostname acme To reset the S9500’s hostname to the default value: acme-> unset hostname
See Also:	get hostname

hsa

Syntax:	**set hsa group <number>** **unset hsa**
Description:	set hsa is used to define high system availability group id. S9500 devices with the same group id will participate in the negotiation process of finding the master for the group. A group id of 0 disables the high system availability feature.
Default:	group id equals to 0.
Example:	To define the high system availability group to 3: ns-> set hsa group 3
See Also:	get hsa
Note:	High availability is only available when the S9500 is running in NAT mode. When an additional S9500 devices join an existing HA group, the master is whichever S9500 device which has the lowest MAC address.

ike

Syntax:	**set ike negotiate <a.b.c.d> type {as | esp}** **set ike preshared <string> <a.b.c.d> <string>** **unset ike preshared <number>**
Description:	set ike is used to define the preshared key for VPN auto IKE definition.
Example:	To define an entry in the IKE preshared key ring for VPN auto definition “autotest” with gateway 172.66.50.1 as “myautokey”: ns-> set ike preshared autotest 172.66.50.1 myautokey To delete a preshared key with id #1 in the IKE key ring: ns-> unset ike preshared 1
See Also:	clear ike, get ike

interface

Syntax:	**set interface {dmz | trust | untrust} bandwidth <number>** **set interface {dmz | trust | untrust} ip <a.b.c.d> <A.B.C.D>** **set interface {dmz | trust | untrust} ping** **set interface {trust | untrust} gateway <a.b.c.d>** **set interface {trust | untrust} mng** **nset interface {dmz | trust | untrust} bandwidth** **unset interface {dmz | trust | untrust} ip** **unset interface {dmz | trust | untrust} ping** **unset interface {trust | untrust} gateway** **unset interface {trust | untrust} mng**
Description:	set interface is used to define the network interface settings. unset interface is used to restore the default settings for the network interfaces. The bandwidth specified is the maximum amount of guaranteed bandwidth available for all policies. The Trusted and Untrusted interfaces use the gateway field to forward packets that don't belong to the network where the S9500 resides. Web management of the S9500 is available by default to the Trusted interface. Remote Web management is accessible to the Untrusted interface by using the mng parameter. However, Web management is not available through the DMZ interface. The ping ability to the S9500 Untrusted interface is disabled by default. Both the DMZ and the Trusted interfaces are pingable. The ping parameter enables the ping ability of an interface.
Default:	Web management through the Trusted interface. Ping ability to both the Trusted and DMZ interfaces. IP addresses, subnet masks, and gateways are 0.0.0.0.
Example:	To define bandwidth for the DMZ interface to 1000 Kilobits per second: ns-> set interface dmz bandwidth 1000 To enable Web management on the Untrusted network interface: ns-> set interface untrust mng To allow the Untrusted interface to be pingable: ns-> set interface untrust ping
See Also:	get interface, unset interface

mip

Syntax:	**set mip <a.b.c.d> host <a.b.c.d> [netmask <A.B.C.D> [modify <a.b.c.d> <A.B.C.D>]]** **unset mip <a.b.c.d> [netmask <A.B.C.D>]**
Description:	set mip is used to define and modify mapped IP configuration. unset mip is used to delete mapped IP configuration. Mapping is allowed for a one-to-one or subnet-to-subnet relationship. When a subnet-to-subnet mapped IP configuration is defined, the subnet mask is applied to both the mapped IP subnet and the original IP subnet.
Example:	To define a one-to-one mapped IP configuration for a machine with IP address 172.16.10.92 to a valid external IP address 205.34.192.1: ns-> set mip 205.34.192.1 172.16.10.92 To define a subnet-to-subnet mapped IP configuration for a subnet with IP address starting from 209.125.15.1 to an original subnet with IP address starting from 10.1.1.1 using a netmask of 255.255.255.252: ns-> set mip 209.125.15.1 10.1.1.1 255.255.255.252 To modify a mapped IP configuration created above to an original subnet address starting from 10.1.1.65 using a netmask of 255.255.255.248: ns-> set mip 209.125.15.1 10.1.1.65 255.255.255.248
See Also:	get mip

policy

Syntax:	**set policy default-permit-all** **set policy {incoming | outgoing | fromdmz | todmz}** **<string> <string> <string>** **{auth | permit | deny | encrypt }** **[count | log | alarm <second-threshold> <minute-threshold>]** **[schedule <name>]** **[traffic gbw <kbps> priority <number> mbw <kbps>]** **unset policy <number>**
Description:	Define a policy which will control traffic in one of 4 ways: authenticate, permit, deny, or encrypt. Traffic from four directions can be specified. There are three strings provided to the command. The first string is the name of the source address. The second string is the name of the destination address. The last string is the name of the service.
Default:	No policy defined.
Example:	To define a policy: ns-> set policy outgoing "Inside Any" "Outside Any" "HTTP" permit log count alarm 10 100 To delete a policy with id #4: ns-> unset policy 4
See Also:	get policy

route

Syntax:	**set route <a.b.c.d> <A.B.C.D> interface {trust|untrust|dmz} [gateway <ip-addr> [metric <number>]]** **unset route <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]**
Description:	Define a static route entry. The gateway (or next hop) IP address is optional; if absent, then the interface default gateway IP address will be used. The metric is optional; if absent, its value is 1. The default interface for all packets with network not specified is the S9500's Untrusted interface.
Default:	One entry for each network interface defined.
Example:	To define a static route for an internal subnet with IP address 172.16.15.0 and subnet mask 255.255.255.0 using an internal router with IP address 172.16.10.4: ns-> set route 172.16.15.0 255.255.255.0 interface trust gateway 172.16.10.4 1
See Also:	get route

scheduler

Syntax:	**set scheduler <string> once <start>** **set scheduler <string> recurrent { monday | tuesday | wednesday | thursday | friday | saturday | sunday } start hh:mm stop hh:mm [start hh:mm stop hh:mm]** **unset scheduler <string> [once | recurrent]**
Description:	set scheduler is used to create and modify scheduler definition.
Example:	To create a scheduler definition named "mytime" which starts from 1/1/1999 11:00AM to 2/2/1999 7:00PM: ns-> set scheduler mytime once start 1/1/1999 11:00 stop 2/2/1999 19:00 To create a scheduler definition named "weekend" which starts from 8:00AM to 5:00PM every Saturday and Sunday: ns-> set scheduler weekend recurrent saturday start 8:00 stop 17:00 ns-> set scheduler weekend recurrent sunday start 8:00 stop 17:00
See Also:	get scheduler

service

Syntax:	**set service <name> clear** **set service <name> protocol [<number>]** **set service <name> [+] protocol tcp src-port <number> dst-port <number>** **set service <name> [+] protocol udp src-port <number> dst-port <number>** **unset service**
Description:	set service is used to add an user defined service. unset service is used to delete user defined service. The first format is used to add the first entry of the service, while the second format is used to append up to 7 additional entries to the named services. The <string> is the name of the defined service. The src or dst keyword is used to define the source and destination port range, where the range is defined as <low number>-<high-number>.
See Also:	get service

syn-threshold

Syntax:	**set syn-threshold <number>** **unset syn-threshold**
Description:	set syn-threshold is used to set the syn-flood protection threshold. The syn-attack firewall protection starts to take effect after the amount of SYN requests to the same location has passed the specified threshold value within 1 second. The S9500 checks this threshold in a one-second interval. Once the amount of SYN requests to the same location has fallen below the threshold, the syn-attack firewall protection is off. When the problem situation happens again, the syn-attack firewall protection turns on again. This parameter has no effect if the syn-attack firewall protection is not enabled. The default threshold value is 200 seconds. The threshold value can be in the range of 0 to 65535.
Default:	200 per second
Example:	To set the syn flood protection threshold to 1000 per second: ns-> set syn-threshold 1000 To reset the syn flood protection threshold to 200 per second: ns-> unset syn-threshold
See Also:	get syn-threshold, get firewall, set/unset firewall

syslog

Syntax:	**set syslog config <a.b.c.d> {auth/sec | local0-7} <facility> <level>** **set syslog { enable | traffic }** **set syslog port <number>** **set syslog webtrend {enable | ip <a.b.c.d> | port <number>}** **unset syslog**
Description:	The syslog mechanism has to be configured before it can be enabled. ■ config: Specify the logging mechanism for the configuration. ■ webtrend: Specify the configuration parameters for the communication with the Webtrends for Firewalls server.
Example:	set syslog enable
See Also:	get syslog

unset all

Syntax:	**unset all**
Description:	Undefined all system information.
Example:	unset all
See Also:	all other set/unset commands

url

Syntax:	**set url config { disable | enable }** **set url message <string>** **set url msg-type <number>** **set url server <ip-addr> <port> <timeout>** **unset url**
Description:	set url is used to define url blocking configuration. URL blocking is provided via WebSense product. This feature can be turned on and off by the config parameter. The origin of the message that is sent to the HTTP client can be specified by the message parameter: 0 from WebTrends and 1 from S9500.
Default:	This feature is disabled. The S9500 message “S9500 and NetPartners WebSENSE have been set to block this site.“ is used. The communication port to WebTrends is 15868 with a timeout value of 10 seconds.
Example:	To enable the url blocking mechanism: ns-> set url config enable To define the url blocking denied message to "This site is blocked": ns-> set url message "This site is blocked" To use the message from the WebSense server: ns-> set url msg-type 0 To specify communication with a WebSense server with IP address 209.44.150.6 at port 15868 and a timeout value of 10 seconds: ns-> set url server 209.44.150.6 25868 10
See Also:	get url

user

Syntax:	**set user + <name> <password>** **set user + <name> dialup <local-spi> <remote-spi> esp null** **set user + <name> dialup <local-spi> <remote-spi>** **esp { 3des | 40-bit-des | des } [key <hex> | password <string>]** **[auth { md5 | sha-1 } key]** **set user timeout <number>** **unset user <string>**
Description:	set user is used to create entry in the user database. unset user is used to delete existing user database entry. There are two types of entries: built-in user database and VPN dialup user. The built-in user database entries are used for authentication while the VPN dialup user entries are used by the IPSec VPN tunnel definition. VPN dialup users having different IPSec parameters can be grouped together and specified by a single VPN policy.
Example:	To create a user definition for a user named “Bill” with password “billp”: ns-> set user + Bill billp
See Also:	get user

vip

Syntax:	**set vip <a.b.c.d> port <number> <string> <a.b.c.d>** **set vip <a.b.c.d> + port <number> <string> <a.b.c.d>** **unset vip <string> port <number>**
Description:	set vip is used to define virtual IP definition. unset vip is used to delete virtual IP definition. The service string after the port number can be any of the 6 services supported: HTTP, FTP, MAIL, POPS, Telnet, or HTTPS.
Example:	To create a virtual IP definition for an S9500 for Untrusted IP address 209.125.11.2 to Trusted IP address 10.1.1.2 for the FTP services running at port 21: ns-> set vip 209.125.11.2 port 21 FTP None 10.1.1.2
See Also:	get vip

vpn

Syntax:	**set vpn <string> manual <local-spi> <remote-spi> gateway <a.b.c.d> esp null auth {md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}}** **set vpn <string> manual <local-spi> <remote-spi> gateway <a.b.c.d> esp {40bit-des {key <64-bit hex> | password <string>} | des {key <64-bit hex> | password <string>} | 3des {key <192-bit hex> | password <string>}} [auth {null | md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}]** **set vpn <string> auto gateway <a.b.c.d> esp null auth {** **set vpn <string> auto gateway <a.b.c.d> esp {40bit-des | des | 3des} [auth {md5 | sha-1}] {kbyte | second} <number>** **unset vpn <string>**
Description:	set vpn is used to create both manual and auto vpn definition. unset vpn is used to delete a vpn definition. The name of the vpn definitions can be up to 20 characters. The manual VPN definition’s local SPI and remote SPI have to be a hex number greater than 3000. Auto VPN definitions use SPI values between 1000 and 2fff. The pre-shared key used by the auto VPN definition can be up to 128 bytes long and it is defined by the “set ike” command.
Default:	Key lifetime is 3600 seconds. The ESP authentication algorithm is NULL when not specified.
Example:	To create a manual VPN definition with name “judy” using DES for ESP encryption and MD5 for ESP authentication and keys are generated by password “judyvpn”. The local and remote SPI are 00001111 and 00002222 and the gateway IP address is 170.45.33.2: ns-> set vpn judy manual 00001111 00002222 gateway 170.45.33.2 esp des password judyvpn auth md5 password judyvpn To create an auto VPN definition with name “mytest” using 3DES for ESP encryption and NULL for ESP authentication with keys’ lifetime of 200 seconds. The gateway IP address is 170.45.33.2 and the preshared key used is “mytest-key”: ns-> set vpn mytest auto gateway 170.45.33.2 esp 3des second 200 ns-> set ike preshared mytest 170.45.33.2 mytestkey
See Also:	get vpn, set/unset ike

Get commands

Get commands are used to show various system configuration parameters and data.

get address

Syntax:	get address [all | dmz | trust | untrust]
Description:	Show address book entries. Each address book entry is shown with these information: id, address, subnet mask, flag, name, and comments.
Example:	To get all the entries in the address book: ns-> get address all To get only address book entries only for the DMZ interface: ns-> get address dmz To get only address book entries only for the Trusted interface: ns-> get address trust To get only address book entries only for the Untrusted interface: ns-> get address untrust
See Also:	set/unset address

get admin

Syntax:	get admin
Description:	Show administrative parameters.
Example:	To show all the administrative parameters of the S9500: ns-> get admin
See Also:	set/unset admin

get alarm

Syntax:	**get alarm [all | event | traffic [policy <id>]]**
Description:	Show alarm entries.
Example:	To show all alarm entries: ns-> get alarm all To show event alarm entries: ns-> get alarm event To show all traffic alarm entries: ns-> get alarm traffic To show traffic alarm entries for a policy with id number 4: ns-> get alarm policy 4
See Also:	set/unset alarm

get arp

Syntax:	**get arp [net]**
Description:	Show entries in the arp table. The output lists all the arp entries existed in the table. It shows the host's IP address, its MAC address, and the interface where it connects to. The if field can be 0, 1, or 2 where 0 is the Trusted interface, 1 is the Untrusted interface, and 2 is the DMZ interface. Each entry has an age timer of 960 seconds. When its age reaches 0, the entry gets deleted off the arp table.
Example:	To show all the entries in the arp table: ns-> get arp
See Also:	set/unset arp

get auth

Syntax:	**get auth [all | queue | settings | table]**
Description:	Show the user authentication settings. A successful authentication attempt causes an entry to be created in the S9500's authentication table. Each entry has a timeout value. Once it reaches the timeout value, the entry is gone and any authentic traffic initiated from the same machine will require authentication. An authentication queue contains a list of authentication requests that are waiting to be processed. This parameter is valid only if the authentication type is the Radius server. An authentication table contains a list of entries that shows where the user initiates the authentication request, how much time is left before the entry gets deleted, and whether the attempt is successful. The S9500 supports a maximum number of 4096 entries in this table. Further attempts will be rejected and retry is necessary. The S9500's user authentication settings contain different information depends on the kind of mechanism being used. When the built-in user database is used, the settings contain only the timeout value for the authenticated entry. With the Radius server authentication mechanism, the settings also contain the Radius server IP address and shared secret. The authentication table shows entries of those machines where the user authentication attempts are originated from. Each entry is numbered and is listed along with the machine's IP address and the amount of time left before the entry gets deleted.
Example:	To show the user authentication settings: ns-> get auth all To show the authentication queue: ns-> get auth queue To show the authentication settings: ns-> get auth settings To show the authentication table: ns-> get auth table
See Also:	clear auth, set/unset auth

get clock

Syntax:	**get clock**
Description:	Show the system clock adjustment. The display includes the current date in calendar format as well as the number of seconds since 1/1/1970 GMT. It also calculates the uptime since the last power up.
Example:	To show the system clock adjustment: ns-> get clock

get config

Syntax:	**get config saved [to tftp <a.b.c.d> <string>]** **get config tftp <a.b.c.d> <string> [to {saved | tftp <a.b.c.d> <string>}]** **get config to {saved | tftp <a.b.c.d> <string>}** **get config size [saved | tftp <a.b.c.d> <string>]**
Description:	Show either the running configuration or a configuration from a specified location. It also provides a mechanism to retrieve a configuration file from one location and save it to another location. ■ saved: Indicates the configuration is retrieved from the flash memory. ■ tftp: Allows retrieval of a specific configuration file from a TFTP server connected to the S9500's Trusted interface. ■ to: Allows saving the retrieved configuration file either to the flash memory or to a TFTP server. ■ size: Shows the size of the configuration file.

Syntax:	**get config saved [to tftp <a.b.c.d> <string>]** **get config tftp <a.b.c.d> <string> [to {saved | tftp <a.b.c.d> <string>}]** **get config to {saved | tftp <a.b.c.d> <string>}** **get config size [saved | tftp <a.b.c.d> <string>]**
Example:	To show the running configuration: ns-> get config To show the configuration that has been saved in the flash memory: ns-> get config saved To show a configuration file named "myconfig" from a TFTP server with IP address 154.30.9.13: ns-> get config tftp 154.30.9.13 myconfig To retrieve a configuration file named "myconfig" from a TFTP server with IP address 154.30.9.13 and save it to the flash memory: ns-> get config tftp 154.30.9.13 myconfig to saved To retrieve a configuration file named "November" and save it as a file named "December" at a TFTP server with IP address 154.30.9.13: ns-> get config tftp 154.30.9.13 November to tftp 154.30.9.13 December To retrieve a configuration file named "myconfig" at a TFTP server with IP address 154.30.9.13 and save it as a file named "yourconfig" at a TFTP server with IP address 209.125.10.2: ns-> get config tftp 154.30.9.13 myconfig to tftp 209.125.10.2 yourconfig To get the size of the configuration file in the flash memory: ns-> get config size saved To get the size of the configuration file named dec1019 from a tftp server with IP address 100.23.44.1: ns-> get config size tftp 100.23.44.1 dec1019
See Also:	save

get console

Syntax:	**get console**
Description:	Show the console parameters. The console idle timeout value and the number of lines displayed per screen is shown. It also tells where debug messages are displayed. The information also lists the number of active connections to the S9500 either through the console or by Telnet. The duration of the connections is also displayed. If it is a Telnet connection, the client machine's IP address is shown whenever possible.
Example:	To show all the console parameters: ns-> get console
See Also:	set/unset console

get counter

Syntax:	**get counter [all | flow | interface]**
Description:	Display the total packet count for any firewall attacks or system network-related packets or the total packet count for each interface or network-related information. The count is cumulative from power-up.
Example:	To display all counters: ns-> get counter all To display counters for firewall attacks or system-related packets: ns-> get counter flow To display counters for the interfaces and network-related information: ns-> get counter int

get dbuf

Syntax:	**get dbuf { info [number] | mem [number] | stream [number]}**
Description:	get dbuf is used to display information and content of the debug buffer. The buffer content can be displayed in raw data by the mem parameter. A formatted output can be retrieved by the stream parameter.
Example:	To display information about the debug buffer: ns-> get dbuf info To obtain a memory dump of the debug buffer at offset 20% from the beginning: ns-> get dbuf mem 20 To obtain a list of the messages in the debug buffer: ns-> get dbuf stream
See Also:	clear dbuf, set console

get debug

Syntax:	**get debug**
Description:	Show the current debug level settings.
Example:	To show the current debug level settings: ns-> get debug
See Also:	debug

get dialup-group

Syntax:	**get dialup-group [all | id <number>]**
Description:	get dialup-group is used to show dialup-up group configuration. ■ all: shows id, name, and total number of members of all defined dialup groups. ■ id: shows detailed information about a defined dialup group. Information about member is shown: its name, SPI values, SA values, ESP encryption, and authentication algorithms along with keys used.
Example:	To show all dialup-group configuration: ns-> get dialup-up all To show a dialup-group configuration with id number 4: ns-> get dialup-up id 4
See Also:	set/unset dialup-group

get dip

Syntax:	**get dip [all | id <number>]**
Description:	get dip is used to show the dynamic IP configuration.
Example:	To show all dip configuration: ns-> get dip all To show a dip configuration with id number 4: ns-> get dip id 4
See Also:	set/unset dip

get file

Syntax:	get file [<string>]
Description:	Show information for files stored in flash memory. It shows which device the file is stored to along with its file name. Currently, the only device supported is the flash memory.
Example:	To show information for file named corpnet from the flash memory: ns-> get file corpnet
See Also:	clear file, save

get firewall

Syntax:	get firewall
Description:	Show firewall attack protection settings.
Example:	To show the firewall attack protection settings: ns-> get firewall
See Also:	set/unset firewall

get global

Syntax:	get global
Description:	Show the global management settings
Example:	To show the global management settings: ns-> get global
See Also:	set/unset global

get hostname

Syntax:	**get hostname**
Description:	Show the name of the S9500 device
Example:	To show the name of the S9500 device: ns-> get hostname
See Also:	set/unset hostname

get hsa

Syntax:	**get hsa**
Description:	Show high availability group information. The information shows which high availability group this S9500 participates in and whether it is currently a master or slave. A group id of 0 turns off the high availability function.
Example:	To show the high availability group information: ns-> get hsa
See Also:	set/unset hsa

get ike

Syntax:	**get ike {conn-entry | cookies | ring}**
Description:	Show current connections, cookies and preshared keys ring for IKE.
Example:	To show all the current IKE connections: ns-> get ike conn-entry To show all IKE cookies: ns-> get ike cookies To show all preshared keys in the IKE ring: ns-> get ike ring
See Also:	set/unset ike, clear ike

get interface

Syntax:	**get interface**
Description:	Show the network interface settings. The System IP is the IP address that is used to administrate the system through the Web management interface or Telnet protocol. The Web management interface port number is shown as well. The Admin IP address specifies either a single machine or a network of machines where the administrator can bring up the Web management interface. User name is the login name used by the administrator to log on to the S9500 before performing any administrative work through the Web management interface or Telnet protocol. Each interface is shown with its MAC address, IP address, and subnet mask. The status of the interface is also shown along with the speed obtained through auto-sensing. The ping ability of each interface is displayed too. The Manage IP address indicates the IP address used for performing Web management from a specific interface. The Gateways used by the Trusted and Untrusted interface are shown by their IP addresses and subnet masks.
Example:	To show information for all network interfaces: ns-> get interface
See Also:	set/unset interface

get log

Syntax:	**get log [all | policy <number>]**
Description:	Show all entries in the log table.
Example:	To show all entries in the log table: ns-> get log all To show the entries in the log table for policy id #3: ns-> get log policy 3
See Also:	clear log

get mac-learn

Syntax:	**get mac-learn**
Description:	Show all entries in the MAC learning table.
Example:	To show all entries in the mac learning table: ns-> get mac-learn
See Also:	clear mac-learn

get mip

Syntax:	**get mip [cache]**
Description:	Show all the mapped IP configuration.
Example:	To show all mapped IP configuration: ns-> get mip
See Also:	set/unset mip

get policy

Syntax:	**get policy [all | incoming | outgoing | todmz | fromdmz | id <number>]**
Description:	Show policy configuration. If a specific policy id is provided, more detail information about the policy is shown. Otherwise, the policy information is shown in the summary format. Policies can be listed for a specific interface by specify the interface named with the get policy command. The all parameter lists policies for all interfaces.
Example:	To show all policy configuration: ns-> get policy all To show all incoming policy configuration: ns-> get policy incoming To show detail information for a policy with id number 5: ns-> get policy id 5
See Also:	set/unset policy

get route

Syntax:	**get route [all | cache | ip <a.b.c.d>}**
Description:	Show the route configuration: IP address, Netmask, Int, Gateway, Metric Flag Memory. Get route with a specific IP address will display the route information as <ip-addr>=><interface>/<gateway>,<hop count>. This can be used as a tool to find out if the packet with particular IP address get routed by the S9500 to the correct interface.
Example:	To show all the route configuration: ns-> get route To show the route information for a machine with IP address of 24.1.60.1: ns-> get route ip 24.1.60.1
See Also:	set/unset route

get sa

Syntax:	**get sa [all | id <number>]**
Description:	Show the IPSec security association entries.
Example:	To show all the IPsec security association entries: ns-> get sa all To show a specific IPsec security association entry with id number 5: ns-> get sa id 5
See Also:	set/unset sa

get scheduler

Syntax:	**get scheduler [all | id <number>]**
Description:	Show the scheduler definition. Each schedule defined has been assigned with an id number.
Example:	To show all the scheduler definitions: ns-> get scheduler all To show a specific scheduler definition with id number 0: ns-> get scheduler id 0
See Also:	set/unset scheduler

get service

Syntax:	**get service [all | system-defined <string> | user-defined <string>]**
Description:	Show one or all service entries.
Example:	To show all service definitions: ns-> get service all To show all system-defined service definitions: ns-> get service system-defined To show all user-defined service definitions: ns-> get service user To show a specific system-defined service called ftp: ns-> get service system-defined ftp
See Also:	set/unset service

get session

Syntax:	**get session [ip { protocol <number> [port <number>] }]** **get session [ip { port <number> }]** **get session [protocol <number> [port <number>]]** **get session [port <number>]**
Description:	Show all entries in the session table. The output indicates whether the S9500 is running in NAT mode. It displays the Trusted and Untrusted IP addresses along with the number of active sessions and the maximum number of simultaneous sessions supported. The number is 4096.
Example:	To get all entries in the session table: ns-> get session To get all entries in the session table for an IP address: ns-> get session ip 172.16.10.92 To get all entries in the session table for port 80: ns-> get session port 80 To get all entries in the session table for protocol 5: ns-> get session protocol 5
See Also:	clear session

get syslog

Syntax:	**get syslog [config | enable | port | traffic | webtrends]**
Description:	Show syslog configuration.
Example:	To show all syslog configuration: ns-> get syslog To show whether syslog mechanism has been configured: ns-> get syslog config To show whether syslog mechanism is enabled: ns-> get syslog enable To show the port that is used to communicated with the syslog server: ns-> get syslog port To show if sending the traffic log through syslog is enabled: ns-> get syslog traffic To show if communication with Webtrends is enabled: ns-> get syslog webtrends
See Also:	set/unset syslog

get system

Syntax:	**get system**
Description:	Show the general system information.
Example:	To show the general system information: ns-> get system
See Also:	set/unset admin, set/unset interface

get tech-support

Syntax:	**get tech-support**
Description:	Show system information for technical support purpose.
Example:	ns-> tech-support

get url

Syntax:	**get url**
Description:	Show the url blocking configuration. The S9500 monitors the status of the WebSense server once a minute. If the WebSense server doesn't respond, the situation is reported in the Web administration interface and all URL requests are blocked. All sessions waiting to be acknowledged by the WebSense server are listed by the order the request is received. The waiting queue can have a maximum of 256 requests.
Example:	ns-> get url
See Also:	set/unset url

get user

Syntax:	**get user [all | id <number>]**
Description:	Show user database info. Each user entry shows the ID assigned, the user name, and whether the account is enabled (1) or disabled (0).
Example:	To show all the entries in the user database: ns-> get user all To show a particular user entry with id 1: ns-> get user id 1
See Also:	set/unset user

get vip

Syntax:	**get vip [all]**
Description:	Show virtual IP info. The algorithm for load balancing is shown along with the status of the servers for each vip defined.
Example:	ns-> get vip
See Also:	set/unset vip

get vpn

Syntax:	**get vpn [all | manual | auto]** **get vpn name <string>**
Description:	Show all VPN definitions. All VPN definitions will be shown in regards of the kind of key management they use. The auto IKE VPN entries are shown by name, gateway, encryption algorithm, authentication algorithm, and the key lifetime. The manual VPN entries are shown by name, local SPI, remote SPI, and encryption/authentication algorithm.
Example:	To show all VPN definitions: ns-> get vpn To show a VPN definition named "mary-home": ns-> get vpn mary-home To show all auto IKE VPN definitions: ns-> get vpn auto To show all manual IKE VPN definitions: ns-> get vpn manual
See Also:	set/unset vpn

Clear Commands

clear alarm

Syntax:	**clear alarm [all | event | traffic [policy <id>]]**
Description:	Clear entries in the alarm table.
Example:	To clear all entries in the alarm table: ns-> clear alarm all To clear event entries in the alarm table: ns-> clear alarm event To clear traffic alarm for all policies in the alarm table: ns-> clear alarm traffic To clear traffic alarm for a policy with id 4 in the alarm table: ns-> clear alarm traffic policy 4
See Also:	get alarm

clear arp

Syntax:	**clear arp**
Description:	Clear entries in the arp table.
Example:	ns-> clear arp
See Also:	get arp

clear auth

Syntax:	**clear auth table**
Description:	Clear authentication information stored in memory.
Example:	To clear all entries in the authentication table: ns-> clear auth table
See Also:	get authentication, set/unset authentication

clear dbuf

Syntax:	**clear dbuf**
Description:	Clear content of the debug buffer.
Example:	ns-> clear dbuf
See Also:	get dbuf, set/unset console

clear file

Syntax:	**clear file <string>**
Description:	Delete the file named <string> in the flash memory.
Example:	To delete a file named “myconfig” in the flash memory: ns-> clear file myconfig
See Also:	get file

clear ike

Syntax:	**clear ike {<a.b.c.d> | cookies [all]}**
Description:	Clear entries related to IKE.
Example:	To clear all existing IKE information for host 172.2.10.1: ns-> clear ike 172.2.10.1 To clear all existing IKE cookies: ns-> clear ike cookies all
See Also:	set/unset ike, get ike

clear log

Syntax:	**clear log [all | event | traffic [policy <id>]]**
Description:	Clear entries in log table.
Example:	To clear all entries in the log table: ns-> clear log To clear event entries in the log table: ns-> clear log event To clear traffic entries for all policies in the log table: ns-> clear log traffic To clear traffic entries for a policy with id 4 in the log table: ns-> clear log traffic policy 4
See Also:	get log

clear mac-learn

Syntax:	**clear mac-learn**
Description:	Clear entries in MAC learning table.
Example:	ns-> clear mac-learn
See Also:	get mac-learn

clear session

Syntax:	**clear session [all]**
Description:	Clear entries in the session table.
Example:	To clear all entries in the session table: ns-> clear session all
See Also:	get session

clear vpn

Syntax:	**clear vpn ike cookie [all | <a.b.c.d>]**
Description:	Clear entries in the IKE cookie table.
Example:	To clear all entries in the IKE cookie table: ns-> clear vpn ike cookie all To clear entries for IP address 100.2.30.1 in the IKE cookies table: ns-> clear vpn ike cookie all 100.2.30.1
See Also:	get vpn ike cookie

Miscellaneous Commands

save

Syntax:	**save [tftp <ip-addr> <filename>]**
Description:	save is used to save the running configuration to either the S9500's flash memory or to a file at a TFTP server which is connected to the Trusted interface. ■ tftp: Allows saving the running configuration to a file at a TFTP server specified by the IP address. ■ filename: String with printable characters and contains no spaces.
Example:	To save running configuration to the flash memory: ns-> save To save running configuration as a file named "myconfig" to a TFTP server with IP address 184.23.11.9: ns-> save tftp 184.23.11.9 myconfig
See Also:	get config

exit

Syntax:	**exit**
Description:	Exit console (re-login required after that).
Example:	ns-> exit

ping

Syntax:	**ping <a.b.c.d>**
Description:	ping a remote host.
Example:	To ping a host with IP address 209.192.11.2: ns-> ping 209.192.11.2

reset

Syntax:	**reset**
Description:	Reset the system.
Example:	ns-> reset

Appendix C

Technical Specifications and Safety Information

Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4” (w) x 7.9” (d) x 2.1” (h)

Communications interfaces: The Netopia S9500 Security Appliance has three RJ-45 jacks for equipment connections and a DB-25 Console port.

Power requirements

- 12 VDC input
- 1 Amp

Environment

Operating temperature: 10° to +40° C

Storage temperature: 0° to +50° C

Relative storage humidity: 5 to 90% non-condensing

Software and protocols

Standards Compliance. IEEE 802.3, Ethernet

IPsec Compliance.

- RFC 1825 (Security Architecture for the Internet Protocol)
- RFC 1826 (IP Authentication Header)
- RFC 1827 (IP Encapsulating Security Payload)
- RFC 1828 (IP Authentication using Keyed MD5)
- RFC 1829 (The ESP DES-CBC Transform)
- RFC 1851 (The ESP Triple DES Transform)

Agency approvals

North America

Safety Approvals:

- United States – UL: 1950 Third Edition

EMI/RFI:

- FCC Part 15, Class A

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

No User-Serviceable Parts Warning

The Netopia S9500 Security Appliance contains no user-serviceable parts and is housed in a tamper-proof enclosure. Therefore, the chassis should never be opened under any circumstances.

Circuit Breaker (15A) Warning

This product relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).

Index